1 Algebra Basics

§1.1 Systems of Equations

Systems of equations appear in problems among all subjects, so it's essential to know how to solve them. There are generally two ways in which we solve systems of equations: elimination and substitution.

Definition 1.1. **Elimination** is where we combine the results of a system of equations to get a new equation with fewer variables. We will most often use elimination to solve systems of linear equations, which you are probably already familiar with.

Example 1.2. Solve the following system of equations:

$$\begin{aligned} 5x + 6y &= 107 \\ 2x + 3y &= 50. \end{aligned}$$

Solution. Multiplying the second equation by 2, we get that

$$4x + 6y = 100.$$

Subtracting this new equation from the first equation, we eliminate the y variable and we find $x = 7$. Plugging this back into our first equation, we have that $6y = 107 - 35 = 72$, so $y = 12$. Therefore, the solution to the system of equations is $(x, y) = (7, 12)$. ■

Definition 1.3. **Substitution** is where we express one variable in terms of another, and we substitute the result into another equation, effectively eliminating a variable. Substitution can almost always be used, even with more complicated systems with nasty terms.

Example 1.4. Solve the following system of equations:

$$\begin{aligned} x - y &= 2 \\ x^2 = y^2 + 2y &= 40. \end{aligned}$$

Solution. Adding y to both sides of the first equation gives us $x = y + 2$. Substituting $y + 2$ in for x in the second equation gives us

$$(y + 2)^2 + y^2 + 2y = 40.$$

After expanding and rearranging, we can factor the quadratic as $2(y + 6)(y - 3) = 0$. Thus, $y = -6$ or $y = 3$. Since $x = y+2$, our two solutions are $(x, y) = (-4, -6)$ and $(x, y) = (5, 3)$. ■

Of course, systems of equations won't always be so tame, nor will they necessarily have two variables. However, we can still use the general principles of substitution and elimination; it may just take a little more manipulation.

Example 1.5 (AMC 12). If x, y, and z are positive numbers satisfying

$$x + 1/y = 4, \qquad y + 1/z = 1, \qquad \text{and} \qquad z + 1/x = 7/3$$

then what is the value of xyz?

Solution. The most straightforward way to solve this is to substitute in the expressions. Subtracting $\frac{1}{y}$ from both sides of the first equation, we get $x = 4 - \frac{1}{y}$. Substituting this into the last equation, we have that

$$z + \frac{1}{4 - \frac{1}{y}} = \frac{7}{3}.$$

After simplifying the fraction and rearranging, we get

$$z = \frac{7}{3} - \frac{y}{4y - 1}.$$

which yields

$$z = \frac{25y - 7}{12y - 3}.$$

Substituting this in to our second equation, we get that $y + \frac{12y-3}{25y-7} = 1$. Multiplying both sides by $25y - 7$ and rearranging, we get the quadratic

$$25y^2 - 20y + 4 = 0.$$

This factors into $(5y - 2)^2 = 0$, so $y = \frac{2}{5}$. Solving for x and z, we have that $x = \frac{3}{2}$ and $z = \frac{5}{3}$. Thus, the value of xyz is 1. ■

Remark. There's a much cleaner solution — try multiplying all three equations and continue from there!

Sometimes, the equations may not look as nice. After substituting or eliminating, we may end up with an equation just as messy as the original. There might seem to be too little information to solve them! In such situations, we have to get more creative.

Example 1.6. If $x^2 + y^2 + z^2 = 14$ and $x + y + z = 6$, find $xy + xz + yz$.

Solution. We are given three unknowns, but only two equations; we will probably have to somehow introduce $xy + xz + yz$ by manipulating the equations. In such problems, a good strategy is some wishful thinking and persistence.

The first equation contains a sum of squares; how can we get this from the other equations? We might think of squaring the second equation to get x^2, y^2, and z^2 terms and hoping it expands nicely. Indeed, squaring the second equation gives us

$$x^2 + y^2 + z^2 + 2xy + 2xz + 2yz = 36.$$

Subtracting the first equation from this and dividing by 2, we get that $xy + xz + yz = 11$. ■

Remark. This manipulation with $x^2+y^2+z^2$ and $xy+xz+yz$ comes up very often in algebra problems—it's a good trick to remember.

Example 1.7. Solve the following system of equations:

$$3x^2-8xy+4y^2=28$$
$$x^2-3xy+2y^2=56.$$

Solution. Our options here are limited, and the terms look complicated. Looking for numerical coincidences is always a good idea, though; notice that we can multiply the first equation by two to get it equal to the second equation. This will cancel out the constant term. Why is this important?

Well, if we eliminate the constant term, we will have a quadratic in x and y that we can factor, giving us a relation between x and y after we use the zero product property. We'll demonstrate that now. Multiplying the first equation by 2 and setting the two equations equal, we have

$$6x^2-16xy+8y^2=x^2-3xy+2y$$

Rearranging all the terms to one side gives us

$$5x^2-13xy+6y^2=0$$

we can treat the equation as a quadratic in terms of x with y being constant. Factoring yields $(x-2y)(5x-3y)=0$—we can get this by noting that if we were to factor the expression on the left-hand-side into two binomials, one would have an x and the other would have a $5x$, so we could test out possibilities for y.

This gives us two possibilities: either $x=2y$ or $x=\frac{3}{5}y$. Now we can plug both possibilities into the first equation.

Setting $x=2y$ into our first equation, we get that $3(2y)^2-8(2y)y+4y^2=28$, which yields $0=28$. Thus the case $x=2y$ gives no solutions. Setting $x=\frac{3}{5}y$, we get that $\frac{7}{25}y^2=28$, which yields $y=\pm 10$. This gives us the solutions $(x,y)=(6,10),(-6,-10)$. Both pairs satisfy our original equations, so we are done. ■

In this problem, we dealt with the given information by finding a quadratic that we could factor. This is a common strategy in algebra problems. Try the following exercise, and look for a way to make it a quadratic!

Exercise 1.8. Solve $4^x+5\cdot 6^x+6\cdot 9^x=0$.

Example 1.9 (Brilliant). Solve the system of equations:

$$x^2+xy=20$$
$$y^2+xy=30.$$

Solution. Looking at the two equations individually doesn't seem to be too helpful. However, if we add the two equations together, we can again get a quadratic in x and y. We get x^2+

$2xy + y^2 = 50$, which factors into $(x + y)^2 = 50$. This looks like a good start, but we still need more information.

Since we added the two equations initially, we might consider subtracting them, too. Indeed, subtraction cancels the xy-terms, yielding $y^2 - x^2 = 10$, which factors into $(y + x)(y - x) = 10$.

Notice that the two equations we obtained share a $(x+y)$ factor, which motivates us to divide them. Dividing the first equation by the second gives us $\frac{x+y}{y-x} = 5$, so $y = \frac{3}{2}x$. Substituting this into our $(x + y)^2 = 50$ equation, we obtain

$$\frac{25}{4}x^2 = 50.$$

so $x = 2\sqrt{2}, -2\sqrt{2}$. Thus, our two solutions are $(x, y) = (2\sqrt{2}, 3\sqrt{2}), (-2\sqrt{2}, -3\sqrt{2})$. Plugging these in, our original equations both hold, so we are done. ■

Let's end with a harder example.

Example 1.10 (2010 AIME I)**.** Let (a, b, c) be the real solution of the system of equations $x^3 - xyz = 2$, $y^3 - xyz = 6$, $z^3 - xyz = 20$. The greatest possible value of $a^3 + b^3 + c^3$ can be written in the form $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

Solution. Given that we're trying to find a value for $a^3 + b^3 + c^3$, the most obvious first thing to consider doing is rewriting the equations as

$$\begin{aligned} a^3 &= 2 + abc \\ b^3 &= 6 + abc \\ c^3 &= 20 + abc. \end{aligned}$$

So $a^3 + b^3 + c^3 = 28 + 3abc$, and we're looking for abc, essentially. Therefore we make the substitution $abc = n$, yielding

$$\begin{aligned} a^3 &= 2 + n \\ b^3 &= 6 + n \\ c^3 &= 20 + n. \end{aligned}$$

Our next step should make a lot of sense: it's hard to deal with one equation at once, but if we multiply them all and use $abc = n$, we get

$$n^3 = (n + 2)(n + 6)(n + 20).$$

This is actually a quadratic — the n^3 terms cancel out. Solving it yields $n = -\frac{15}{7}, -4$ as solutions; from here, given that we're actually looking for the maximum possible value of $a^3 + b^3 + c^3$, we plug in $n = abc = -\frac{15}{7}$, yielding an answer of $\frac{151}{7}$. In the form the question asks for, our answer is $151 + 7 = 158$, and we are done. ■

That was a tough problem, and we had to use a lot of tools to solve it. The key steps were figuring out we only needed to find abc, then rearranging the equations to get a polynomial in abc.

Remark. A recurring theme throughout all our examples is that if you don't see the solution immediately, mess around with the givens, and eventually you will get a useful equation. Look for expressions that could be key to solving the problem, like a difference of squares. If you have more variables in equations, then don't try to solve for individual values directly; maybe you can't get an equation only in terms of a, but maybe you can get an equation in terms of just $a+b$ or ab.

Exercise 1.11. Solve the system of equations.

$$\begin{cases} a+b+c=7 \\ b+c+d=6 \\ c+d+a=9 \\ d+a+b=8 \end{cases}$$

Exercise 1.12 (ARML 1990). If $a+b=c, b+c=d, c+d=a$, and b is a positive integer, compute the greatest possible value for $a+b+c+d$.

Exercise 1.13. Solve the following system of equations:

$$\begin{aligned} x^2-6y &= 7 \\ y^2-10x+41 &= 0. \end{aligned}$$

§1.2 Mean, Median, and Mode

We learn the definitions of mean, median, and mode early on in school, but here we'll review them in detail. Mean, median, and mode problems usually appear early in the AMC and are generally quite simple. It would be a shame to ignore these concepts and miss very easy points!

Definition 1.14. The **mean**, or average, of a set of numbers is equal to the total sum of all of the numbers, divided by however many numbers are in the set. More succinctly, for numbers $a_1, a_2, ..., a_n$, the mean is equal to

$$\frac{a_1+a_2+\cdots+a_n}{n}.$$

One can find the **median** of a set of numbers by ordering the numbers in increasing order, then finding the number in the middle. If there is an even number of numbers, then the median is found by taking the mean of the middle two numbers. For example, the median of $\{1,3,5\}$ is 3, while the median of $\{1,3,5,6\}$ is $\frac{3+5}{2}=4$.

The **mode** is the number that appears most frequently in a set of numbers. We can have one or multiple modes. For example, the unique mode of $\{1,2,2,4\}$ is 2 while $\{1,1,2,2,4\}$ has two modes, 1 and 2.

Let's get right into the examples.

Example 1.15 (2016 AMC 10). The mean, median, and mode of the 7 data values

$$60, 100, x, 40, 50, 200, 90$$

are all equal to x. What is the value of x?

Solution. The mean is equal to the total sum, divided by 7. Also, we're given that this mean is equal to x, so we can write

$$\frac{60+100+x+40+50+200+90}{7} = x \implies \frac{540+x}{7} = x.$$

Hence, $540+x = 7x$, so $x = 90$. Indeed, if $x = 90$, then the mode and median of the numbers are both 90, we can be sure that we're right. ■

Example 1.16 (2019 AMC 12B)**.** What is the sum of all real numbers x for which the median of the numbers $4, 6, 8, 17$, and x is equal to the mean of those five numbers?

Solution. In terms of x, the mean of the set is

$$\frac{4+6+8+17+x}{5} = \frac{x+35}{5}$$

The median, however, can take three values, depending on the value of x.

1. If $x \geq 8$, then 8 is the median.
2. If $x \leq 6$, then 6 is the median.
3. If $6 < x < 8$, then x is the median.

Make sure to verify our above claims for yourself! Now, we can take each of them on case at a time.

1. $\frac{x+35}{5} = 8$, so $x = 5$.
2. $\frac{x+35}{5} = 6$, so $x = -5$.
3. $\frac{x+35}{5} = x$, so $x = 8.75$.

However, we cannot simply conclude that our answer is $5-5+\frac{35}{4} = \frac{35}{4}$. We first have to check that that the solutions satisfied the conditions for each case.

Let's look at case 1: Does it make sense? Notice that we said that $x \geq 8$, but our solution was $x = 5$, a contradiction. So this case doesn't actually work.

The second case clearly works, as $x = -5 \leq 6$. The third case is invalid because 8.75 is not between 6 and 8. Thus, our answer is just -5. ■

Example 1.17 (2017 AMC 10B)**.** Last year Isabella took 7 math tests and received 7 different scores, each an integer between 91 and 100, inclusive. After each test she noticed that the average of her test scores was an integer. Her score on the seventh test was 95. What was her score on the sixth test?

Solution. First, let's make use of the divisibility condition: the sum of all seven scores must be divisible by 7, as we're given that the average of Isabelle's scores is an integer. The largest possible sum of scores is

$$100+99+98+97+96+95+94 = 679 = 7(97).$$

The smallest possible sum is

$$91 + 92 + 93 + 94 + 95 + 96 + 97 = 658 = 7(94).$$

This means that the only possible sum of scores of all seven tests are 7(94), 7(95), 7(96), and 7(97), or 658, 665, 672, and 679 respectively.

In order to get the sum of the first six test scores, we can subtract 95 from each, getting 563, 570, 577, and 584. The sum should be divisible by 6, since the average of the first 6 test scores is an integer. 570 is the only one of these integers divisible by 6. Thus, 570 is the sum of the first six test scores.

Now, note that the sum of the first five scores must be divisible by 5. Thus, if 570 minus a test score yields a multiple of five, then that test score must be a multiple of five, namely either 95 or 100. Since all scores must be different, 95 can't be used, so the sixth test score is 100. ■

Example 1.18 (2019 AMC 10A). Melanie computes the mean μ, the median M, and the modes of the 365 values that are the dates in the months of 2019. Thus her data consists of 12 1s, 12 2s, . . . , 12 28s, 11 29s, 11 30s, and 7 31s. Let d be the median of the modes. Which of the following statements is true?

(A) $\mu < d < M$
(B) $M < d < \mu$
(C) $d = M = \mu$
(D) $d < M < \mu$
(E) $d < \mu < M$

Solution. Let's try to determine what is easy to solve for first. In most cases (including this problem), the mode is easiest to determine. There are 28 of them, since the numbers $1, 2, 3, ...28$ all appear 12 times each, making each the most common. Thus, $d = 14.5$.

Now let's locate the median. Since there are 365 values, the middle value is the 183rd one. Thus we can determine the 183rd smallest value by counting up by 12s starting from 1. As $12 \cdot 15 = 180$, it follows that the median M is 16, as the 183rd day would appear in a group of 16s.

Determining how big the mean is takes some ingenuity. Direct computation seems difficult, so let's do something more clever. Assume that every month had 31 days—then the mean would clearly be 16. But since some months have less than 31 days, the mean must be less than 16, so $\mu < M$.

Lastly, let's compare μ and d. Note that if every month had 28 days, then μ would be equal to 14.5; however, there are more days than that in some months. Therefore $d < \mu$.

It thus follows that $d < \mu < M$, and choice (E) is our answer. ■

Remark. Two strategies come to mind as we solved the above problem:

1. We never actually computed the exact value of μ; we just found it relative to d and M. This was crucial, as computing the mean would be incredibly time-consuming. It is important to note that you don't always have to find exact values if the question doesn't ask for them.
2. We also solved similar but easier problems to help us gain insights on the original problem (like considering if all months had 31 and 28 days.) This strategy is almost always helpful, too.

Exercise 1.19. Suppose that A and B are disjoint sets. Assume set A has three elements that have a mean of 7, and set B has four elements that have a mean of 8. What is the mean of the 7 elements in the union of A and B?

Exercise 1.20 (2000 AMC 12). When the mean, median, and mode of the list

$$10, 2, 5, 2, 4, 2, x$$

are arranged in increasing order, they form a non-constant arithmetic progression. What is the sum of all possible real values of x?

§1.3 Rate Problems

Rate problems are especially common in math competitions and can be quite tricky without practice. They usually require making an observation about a system of moving objects. Typically, the three quantities to pay attention to are time (t), speed (r), and distance (d). These have a special relationship:

$$d = rt.$$

Often, this equation can help find an unknown quantity if two quantities are known and the other one isn't. Note that r can be any kind of rate, from miles traveled per hour to the number of books read in a day.

Make sure that you convert units accordingly! For example, if the rate is in mph, make sure that distance is in miles and time in hours.

Example 1.21 (2018 AMC 10B). Sam drove 96 miles in 90 minutes. His average speed during the first 30 minutes was 60 mph (miles per hour), and his average speed during the second 30 minutes was 65 mph. What was his average speed, in mph, during the last 30 minutes?

Solution. During the first 0.5 hours, Sam's average speed was 60 mph. Using $d = rt$, his distance traveled was $60 \times 0.5 = 30$ miles during the first 30 minutes. During the second 30 minutes, using $d = rt$, we get that Sam traveled $65 \times 0.5 = 32.5$ miles.

We are given that during all of the 90 minutes, Sam traveled 96 miles. Thus, he traveled $96 - 30 - 32.5 = 33.5$ miles total in the last half-hour. Thus, his speed then was $d/t = 33.5/0.5 = 67$ mph. ■

Example 1.22. Peter drives to work in the morning at an average speed of 30 mph. He gets hungry at night so he drives quicker on the way back home, at an average speed of 45 mph. Assume he takes the same route going to and coming back from his work place. If the combined time taken for this back-and-forth trip is 1 hour, how long does it take for him to drive to work in the morning, in minutes?

Solution. Let the time in hours that Peter takes to drive to work in the morning be t_1, and let the time in hours that Peter takes to drive back home at night be t_2. We know that $t_1 + t_2 = 1$ — note that we selected *hours* as our unit because the speeds we're given are in mph. Let the distance between his home and work be d. Then, we have $d = 30t_1$ for the morning commute and $d = 45t_2$ for the night trip.

Rearranging these equations, we get $t_1 = \frac{d}{30}$ and $t_2 = \frac{d}{45}$. Substituting this into our first equation gives us

$$t_1 + t_2 = \frac{d}{30} + \frac{d}{45} = 1 \implies d\left(\frac{1}{30} + \frac{1}{45}\right) = 1 \implies \frac{d}{18} = 1 \implies d = 18.$$

To finish, we go back to the question. It's asking us to find t_1, so we plug in d into our equation for t_1, to get $t_1 = \frac{18}{30}$ hours or $t_1 = 36$ minutes. ■

This next problem shows up very often in competitions in different forms, so make sure to understand what is going on.

Example 1.23. It takes Alice 3 hours to complete a job. It takes Bill 7 hours to complete the same job. If the two collaborate on this job, how long will it take for the job to be completed?

Solution. If it takes Alice 3 hours to complete a job, this means that in 1 hour, she completes $\frac{1}{3}$ of the job. Similarly, in 1 hour, Bob completes $\frac{1}{7}$ of his job. This means that if both of them work together, they can complete

$$\frac{1}{3} + \frac{1}{7} = \frac{10}{21}$$

of the job in 1 hour. This means that to complete the job, it takes both of them $\frac{21}{10}$ hours. ■

Rate problems generally just boil down to identifying what quantity is represented by each of the variables d, r, and t, then applying $d = rt$ as necessary.

Exercise 1.24 (2007 AIME I). A 100 foot long moving walkway moves at a constant rate of 6 feet per second. Al steps onto the start of the walkway and stands. Bob steps onto the start of the walkway two seconds later and strolls forward along the walkway at a constant rate of 2 feet per second. Two seconds after that, Cy reaches the start of the walkway and walks briskly forward beside the walkway at a constant rate of 4 feet per second. At a certain time, one of these three persons is exactly halfway between the other two. At that time, find the distance in feet between the start of the walkway and the middle person.

Exercise 1.25 (1951 AHSME). Tom, Dick and Harry started out on a 100-mile journey. Tom and Harry went by automobile at the rate of 25 mph, while Dick walked at the rate of 5 mph. After a certain distance, Harry got off and walked on at 5 mph, while Tom went back for Dick and got him to the destination at the same time that Harry arrived. How many hours did the trip take?

§1.4 Absolute Value

Definition 1.26. The **absolute value** of a real number x, denoted by $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{for } x \geq 0, \\ -x & \text{for } x < 0. \end{cases}$$

Note: We will only deal with real numbers in this section. $|x|$ has a different meaning when x is a complex number, which will be defined on Day 5.

When dealing with a problem involving absolute values, the most common approach in AMC and early AIME is to use casework with two cases: either the expression between the absolute value signs is negative, or it is nonnegative.

Example 1.27 (2004 AMC 10A)**.** What is the value of x if $|x-1| = |x-2|$?

Solution. We have two cases:

1. Both $|x-1|$ and $|x-2|$ are greater than or equal to 0, or both are less than or equal to zero. Then equation simplifies to $x-1 = x-2$. This gives us $-1 = -2$, which is a contradiction. Thus, we know only one expression is positive, while the other is negative.
2. Either $|x-1|$ or $|x-2|$ is positive, the other is negative. The equation simplifies to $x-1 = 2-x$, so $x = \frac{3}{2}$.

It follows that our only working value is $x = \frac{3}{2}$, so that is our answer. ■

Example 1.28 (2011 AMC 12A)**.** Suppose that $|x+y|+|x-y| = 2$. What is the maximum possible value of $x^2 - 6x + y^2$?

Solution. We have four cases this time, and these cases include all of the possible values of x and y.

1. $(x+y)+(x-y) = 2$ yields $x = 1$. Note that this case also forces y to lie between -1 and 1.
2. $-(x+y)-(x-y) = 2$ yields $x = -1$. Note that this case also forces y to lie between -1 and 1.
3. $(x+y)-(x-y) = 2$ yields $y = 1$. Note that this case also forces x to lie between -1 and 1.
4. $-(x+y)+(x-y) = 2$ yields $y = -1$. Note that this case also forces x to lie between -1 and 1.

These cases imply that $y^2 = 1$ is always the maximum possible value of y^2, and that $x^2 = 1$ is always the maximum possible value of x^2. It turns out, then, that we can just maximize $-6x$ by setting $x = -1$, which yields $x^2 - 6x + y^2 = 8$ for $(x, y) = (-1, 1)$. Note that it is clear that we cannot obtain a number any larger than this, because $-6x$ is maximized at $x = -1$, and x^2 and y^2 both achieve a maximum possible value of 1. ■

Exercise 1.29. Prove the following properties of $|x|$:

1. $|x| = \sqrt{x^2}$
2. $|x| \geq 0$,

3. $|x| = 0 \iff x = 0$,
4. $|xy| = |x||y|$,
5. $|x + y| \leq |x| + |y|$.

Exercise 1.30 (2000 AMC 12 Problem 5). If $|x - 2| = p$, where $x < 2$, then what is $x - p$?

Exercise 1.31. There are exactly N distinct rational numbers k such that $|k| < 200$ and

$$5x^2 + kx + 12 = 0$$

has at least one integer solution for x. What is N?

The absolute value problems in these sections weren't so bad; when graphs are involved, though, they become harder. We'll go over graphs in general as well as absolute value problems involving graphs in the following section.

§1.5 Graphs

Definition 1.32. A **graph** is a visual representation of a function or relation. We will usually obtain a graph from a function like $f(x) = x^2+2x$ by plotting each value of x as the x-coordinate and the corresponding value of $f(x)$ as the y-coordinate of a point on the xy-plane.

In this section, we will be looking at the graphs of several different types of equations. In a graph, the x and y-axes separate the plane into 4 regions. The top right is called the first quadrant, the top left is the second quadrant, the bottom left is the third quadrant, and the bottom right is the fourth quadrant.

§1.5.1 Lines

When we are graphing lines, there are two common forms: point-slope form and the slope-intercept form.

Given a point on the line and that line's slope, we can use **point-slope form**. If the point we are given is (x_0, y_0) and its slope is m, then the equation of the line is

$$y - y_0 = m(x - x_0).$$

For example, the line passing through $(2, 5)$ with slope $\frac{1}{2}$ has equation $y - 5 = \frac{1}{2}(x - 2)$.

Slope-intercept form is the more commonly used of the two forms; if m is the slope of a line and b is its y-intercept — that is, the line passes through $(0, b)$ — then the equation of the line is

$$y = mx + b.$$

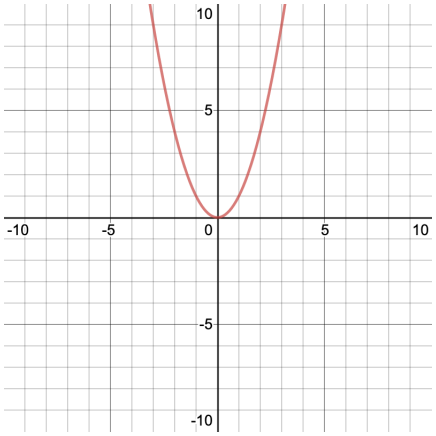
There are two important facts to remember regarding the slopes of lines. First, two lines are parallel if and only if their slopes (m) are equal. Second, two lines are perpendicular if and only if their slopes multiply to -1 (in other words, one slope is the negative of the reciprocal of the other slope.)

§1.5.2 Higher Degree Polynomials and Absolute Value

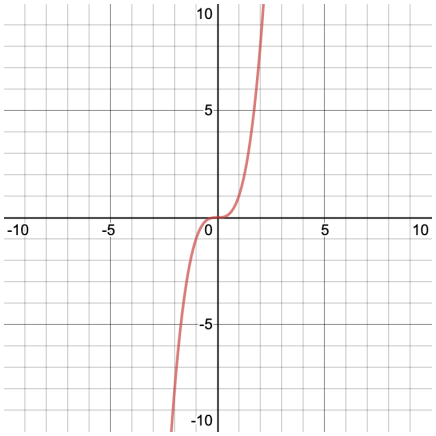
While graphs of higher degree polynomials and absolute values are not seen too often in competitions, it is still good to know what they look like. The most important thing to remember is the relationship between the y and x values, as that is what's going to help you solve the problem. Drawing a diagram can definitely help, but the equation is what truly matters.

With that being said, here are a few graphs that you should know. If you forget what they look like, you can always make a table and plug in values of x to get a rough idea of what graph looks like.

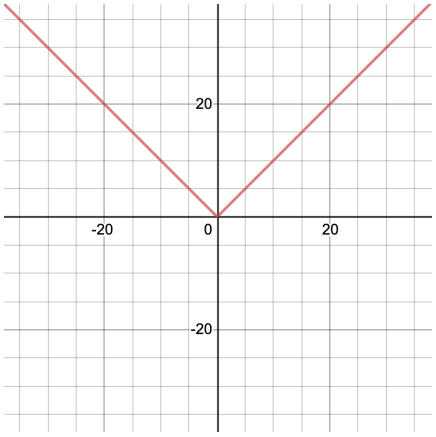
Quadratic ($y = x^2$):



Cubic ($y = x^3$):



Absolute Value ($y = |x|$):



Exercise 1.33. Sketch the graph of $y = x^3 + 3x^2 + 5x + 6$.

Exercise 1.34. Sketch the graph of $y = x^4 + 4x^3 + 2x^2 + 1$.

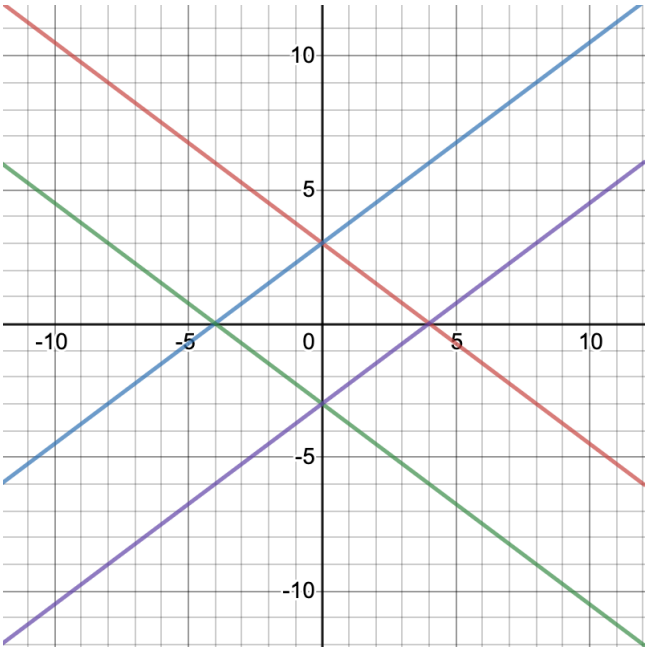
§1.5.3 Example Problems

Example 1.35. (2005 AMC 12B) What is the area enclosed by the graph of $|3x|+|4y| = 12$?

Solution. We begin by using casework, which almost always works when dealing with absolute values.

1. $3x + 4y = 12$ yields $y = -\frac{3}{4}x + 3$
2. $3x - 4y = 12$ yields $y = \frac{3}{4}x - 3$
3. $-3x + 4y = 12$ yields $y = \frac{3}{4}x + 3$
4. $-3y - 4y = 12$ yields $y = -\frac{3}{4}x - 3$

We can graph the equations above (because they are in slope-intercept form) to get:



The area enclosed by the graph of $|3x| + |4y| = 12$ is a rhombus with vertices at $(4, 0)$, $(-4, 0)$, $(0, 3)$, and $(0, -3)$. The area of a rhombus is half the product of its diagonals, which in this case is $\frac{1}{2} \cdot 8 \cdot 6 = 24$. ■

Example 1.36 (2006 AMC 12A). Which of the following describes the graph of the equation $(x + y)^2 = x^2 + y^2$?

(A) the empty set (B) one point (C) two lines (D) a circle (E) the entire plane

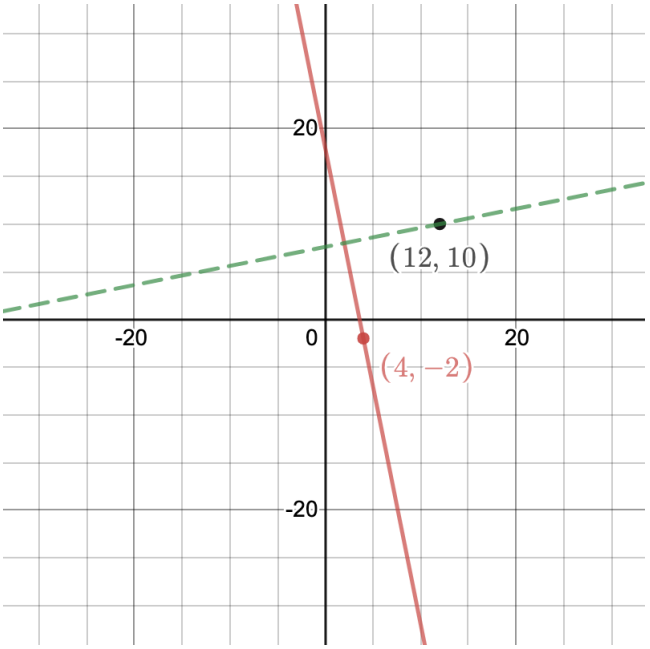
Solution. We begin by simplifying the equation; note that

$$\begin{aligned} x^2 + y^2 &= (x + y)^2 \\ &= x^2 + y^2 + 2xy. \end{aligned}$$

This means that $2xy = 0$. Then either $x = 0$ or $y = 0$, so the graph actually is just the x and y-axes, or two lines. Our answer is (C). ■

Example 1.37 (2007 AMC 12A). A piece of cheese is located at $(12, 10)$ in a coordinate plane. A mouse is at $(4, -2)$ and is running up the line $y = -5x + 18$. At the point (a, b) the mouse starts getting farther from the cheese rather than closer to it. What is $a + b$?

Solution. The hardest part of this problem is figuring out what we actually want. The easiest way to approach this problem is to draw the line $y = -5x + 18$ and label the points $(12, 10)$ and $(4, -2)$.



Let's do a bit of geometry: the mouse is closest to the cheese when it is standing at the foot of the perpendicular from $(12, 10)$ to the mouse's path. Therefore we want to find the intersection of the perpendicular from $(12, 10)$ to $y = -5x + 18$ with the line $y = -5x + 18$.

Calling this perpendicular line ℓ, we note that ℓ has slope $\frac{1}{5}$ by our negative reciprocal rule, and that it passes through $(12, 10)$. Therefore, by point-slope form, the equation of ℓ is

$$y - 10 = \frac{1}{5}(x - 12).$$

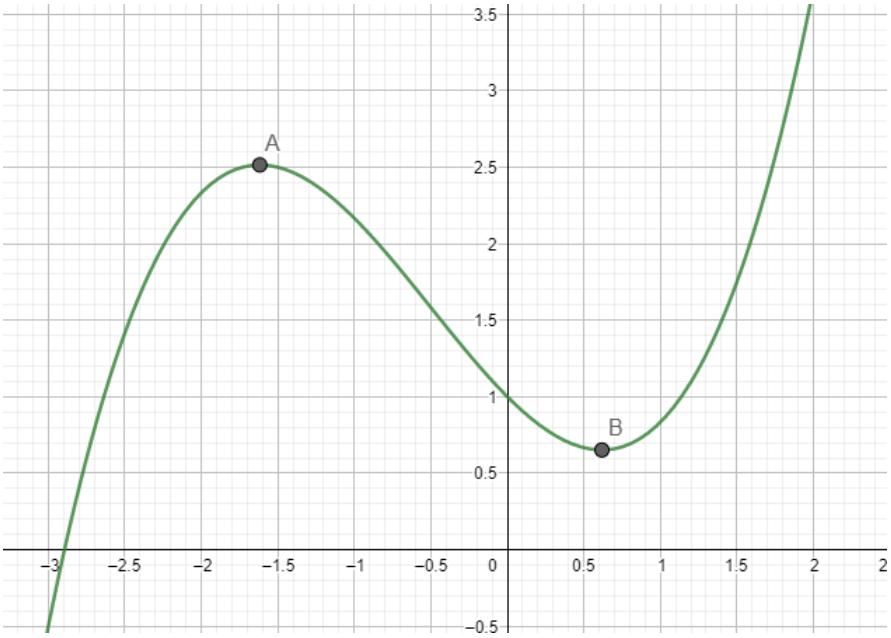
But we already know that the other line has equation $y = -5x + 18$, so this yields a system of two equations. It's possible to solve for their intersection and get $(2, 8)$, so $a = 2$ and $b = 8$ implies that our answer is $2 + 8 = 10$. ■

§1.5.4 Polynomial Graph Intuition

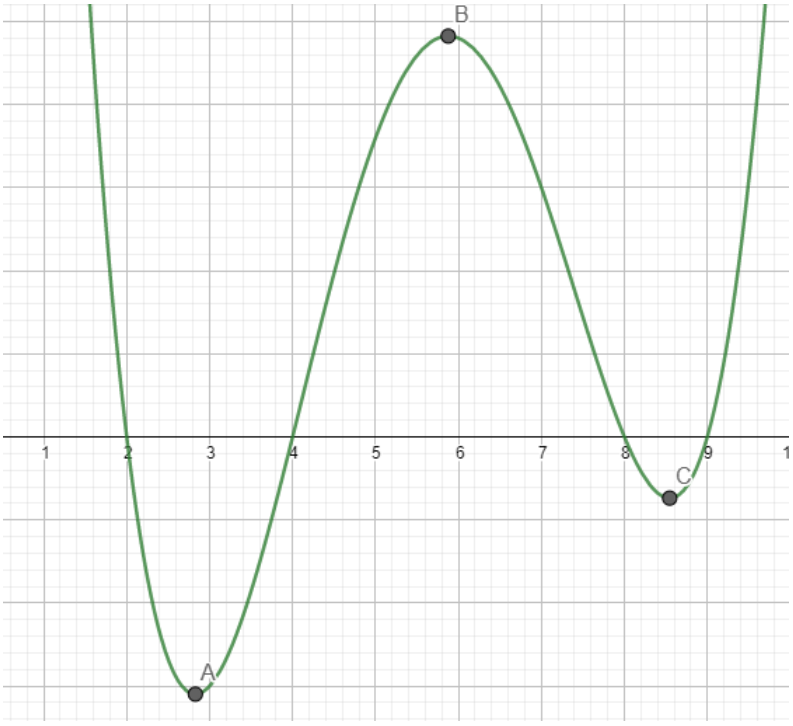
The next problem we tackle requires a lot of graphical intuition, so before we get into it, we'll go over what polynomial graphs tell us.

The first thing we should know is that cubics (also known as third-degree polynomials) have at most two "bends" (extreme values), or two places where the graph changes from increasing to decreasing. The locations at which the graph goes from increasing to decreasing are called local **maxima** (plural of "maximum"), and the locations where the graph goes from decreasing to increasing are called local **minima** (plural of "minimum"). This can be generalized for a n-degree polynomial as well; they have at most $n - 1$ extreme values.

For example, here is a graph of a cubic:



Note that point A is a local maximum and point B is a local minimum. Here's an arbitrary quartic:



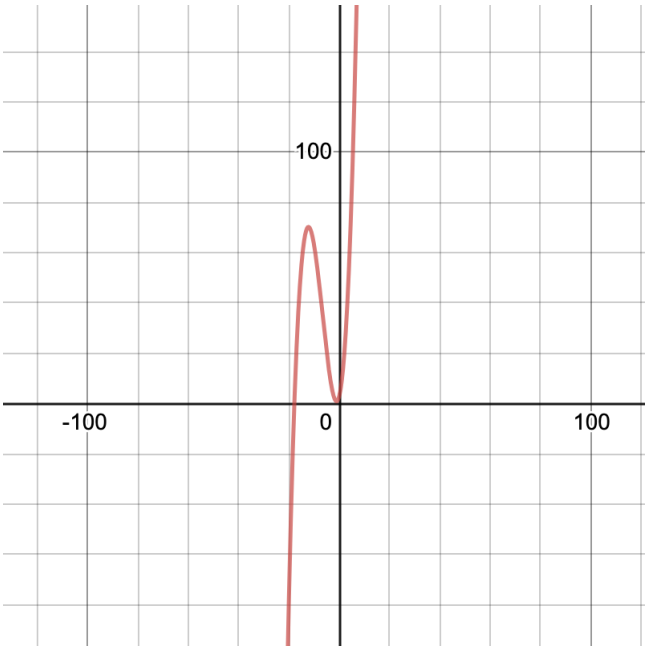
This graph has local minima at points A and C and a local maximum at point B.

Of course, polynomials can have fewer than $n-1$ extreme values, they just can't have more. One such example of a n-degree polynomial with fewer than $n-1$ extreme values is the cubic function $y = x^3$. If you look at the image earlier in the handout, you will realize that it only has one "extreme value", and this value is actually neither a maxima nor a minima!

The reason this is possible is because extreme values are not limited to maxima and minima; they could be neither. The definition we have here for an extreme value is rather vague, for we are not yet equipped with the knowledge to formally define these extreme values (that would have to wait until calculus). However, for now, it's fine if we just think about extreme values as places where the graph of a function "bends," or changes direction.

Another thing to remember is that as the x value of a polynomial with an odd degree approaches infinity, it goes in the opposite direction from where it came from. If the polynomial has an even degree, however, as x approaches infinity, the function travels in the same direction as where it came from. This is known as a polynomial's "end behavior."

Let's take $f(x) = \frac{1}{10}x^3 + 2x^2 + 4x + 3$ as an example. The leading coefficient is $\frac{1}{10}$, which is positive, so we know that $f(x)$ approaches infinity as x gets bigger. $f(x)$ has degree 3, which is odd, so as x gets smaller and smaller, $f(x)$ approaches negative infinity. We can check that this is accurate by taking a look at the graph of this function:



Exercise. Consider $f(x) = x^4 + 3x^2 + 5x + 7$ and $g(x) = -x^5 + 3x^4 + 2x^3 + 10$. What is the end behavior of $f(x)$? What about $g(x)$?

Now that we are armed with this knowledge, we are ready to tackle the next problem.

Example 1.38 (2015 AIME I). Let $f(x)$ be a third-degree polynomial with real coefficients satisfying

$$|f(1)| = |f(2)| = |f(3)| = |f(5)| = |f(6)| = |f(7)| = 12.$$

Find $|f(0)|$.

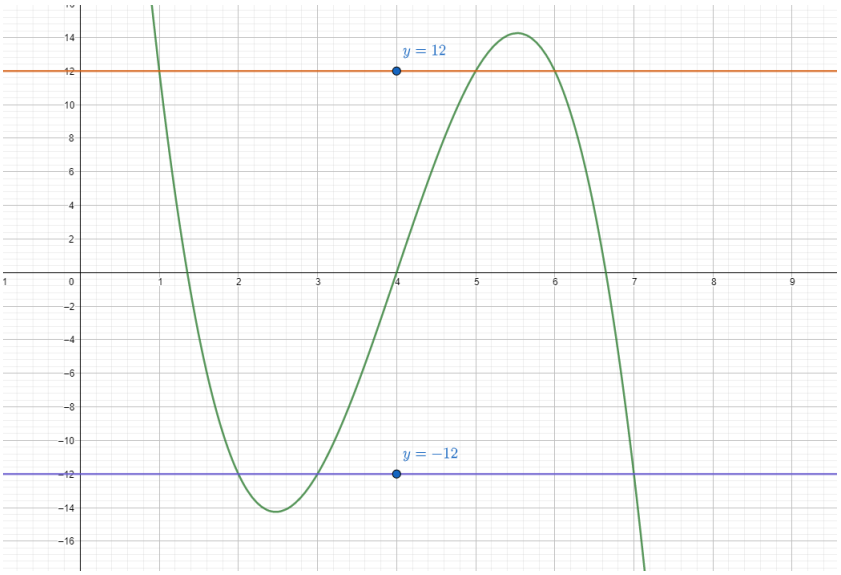
Solution. We are given six values of $|f(x)|$ that are equal. However, only three values of x can give the same value of $f(x)$.

There are two ways we could have deduced that; one way is by drawing a graph and seeing that a horizontal line could not intersect it in more than 3 locations, and the other is by noticing that $f(x) + 12$ and $f(x) - 12$ both have degree 3 and so can have at most 3 roots.

This means that three of the values must be -12, while the other three must be 12. Now, we can assume without loss of generality that the leading coefficient is negative; this shouldn't change our answer since if $f(x)$ satisfies the conditions in the problem, then $-f(x)$ must satisfy them as well, since the problem statement uses absolute value signs.

Now we can graph some arbitrary cubic with positive leading coefficient with six distinct values of x such that $f(x) = \pm 12$.

Consider an arbitrary cubic graph with negative leading coefficient (sketch one out yourself!). There are three regions of interest: label the left of the first bend as A, the region between the first and second bend as B, and the region to the right of the second bend as C (if you drew the graph correctly, $f(x)$ should be decreasing in region A, increasing in region B, and decreasing in region C).



By drawing horizontal lines, it is clear that $f(x) = 12$ exactly once in each region A, B, and C, and the same is true for $f(x) = -12$. Then $x = 1, 2$ are in region A, $x = 3, 5$ are in region B, and $x = 6, 7$ are in region C. From the shape of the graph it is clear that in regions A and C, we have that $f(x) = 12$ before $f(x) = -12$, while the opposite is true in region B. So we have $f(1) = f(5) = f(6) = 12$ while $f(2) = f(3) = f(7) = -12$.

Now, let $f(x) = ax^3 + bx^2 + cx + d$. If we plug in $x = 1, 2, 3, 5, 6, 7$, we get the following

system of equations:

$$\begin{aligned} a+b+c+d &= 12 \\ 8a+4b+2c+d &= -12 \\ 27a+9b+3c+d &= -12 \\ 125a+25b+5c+d &= 12 \\ 216a+36b+6c+d &= 12 \\ 343a+49b+7c+d &= -12 \end{aligned}$$

We have six equations and four variables, so in reality we only need the first four equations to solve for the different values (we could use any four of the six, but the first four have smaller coefficients). Solving the system gives us $d = f(0) = 72$. ■

This was a pretty long and tough problem, but make sure you understand all of the deductions we made using the graph. Visualizing a problem oftentimes leads to much cleaner solutions than focusing only on the algebra.

Exercise 1.39. Finish the solution for the previous question by solving the system of equations.

Exercise 1.40 (1961 AHSME). If the graphs of $2y + x + 3 = 0$ and $3y + ax + 2 = 0$ are to meet at right angles, the what is the value of a?

Exercise 1.41 (2006 AMC 10B). The lines $x = \frac{1}{4}y + a$ and $y = \frac{1}{4}x + b$ intersect at the point $(1, 2)$. What is $a + b$?

Exercise 1.42 (1998 AIME). The graph of $y^2 + 2xy + 40|x| = 400$ partitions the plane into several regions. What is the area of the bounded region?

Exercise 1.43 (2016 AMC 12A). Which of these describes the graph of $x^2(x + y + 1) = y^2(x + y + 1)$?
(A) two parallel lines
(B) two intersecting lines
(C) three lines that all pass through a common point
(D) three lines that do not all pass through a common point
(E) a line and a parabola

§1.6 Homework Problems

Problem 1.1. [3] Kevin runs at a speed of 350 meters per minute and Vincent at a speed of 380 meters per minute. After half an hour, how far apart are Kevin and Vincent assuming they run in opposite directions?

Problem 1.2 (2020 AMC 10B)**.** [5] How many ordered pairs of integers (x, y) satisfy the equation

$$x^{2020} + y^2 = 2y?$$

Problem 1.3 (2001 AIME I)**.** [5]

A finite set $\mathcal{S}$ of distinct real numbers has the following properties: the mean of $\mathcal{S} \cup \{1\}$ is 13 less than the mean of $\mathcal{S}$, and the mean of $\mathcal{S} \cup \{2001\}$ is 27 more than the mean of $\mathcal{S}$. Find the mean of $\mathcal{S}$.

Problem 1.4 (2020 AMC 10A)**.** [5] What is the median of the following list of 4040 numbers?

$$1, 2, 3, ..., 2020, 1^2, 2^2, 3^2, ..., 2020^2$$

Problem 1.5 (2010 HMMT)**.** [5] Suppose that x and y are positive reals such that

$$x - y^2 = 3, \qquad x^2 + y^4 = 13.$$

Find x.

Problem 1.6 (2018 AMC 12A)**.** [5] For positive integers m and n such that $m + 10 < n + 1$, both the mean and the median of the set $\{m, m + 4, m + 10, n + 1, n + 2, 2n\}$ are equal to n. What is $m + n$?

Problem 1.7 (2002 AMC 12A)**.** [5] The mean, median, unique mode, and range of a collection of eight integers are all equal to 8. What is the largest integer that can be an element of this collection?

Problem 1.8 (2018 AMC 10A)**.** [8] Which of the following describes the set of values of a for which the curves $x^2 + y^2 = a^2$ and $y = x^2 - a$ in the real xy-plane intersect at exactly 3 points?

(A) $a = \frac{1}{4}$ **(B)** $\frac{1}{4} < a < \frac{1}{2}$ **(C)** $a > \frac{1}{4}$ **(D)** $a = \frac{1}{2}$ **(E)** $a > \frac{1}{2}$

Problem 1.9 (2016 AMC 10B)**.** [9] What is the area of the region enclosed by the graph of the equation $x^2 + y^2 = |x| + |y|$?

Problem 1.10 (1989 AIME)**.** [10] Assume that $x_1, x_2, \ldots, x_7$ are real numbers such that

$$\begin{aligned} x_1 + 4x_2 + 9x_3 + 16x_4 + 25x_5 + 36x_6 + 49x_7 &= 1 \\ 4x_1 + 9x_2 + 16x_3 + 25x_4 + 36x_5 + 49x_6 + 64x_7 &= 12 \\ 9x_1 + 16x_2 + 25x_3 + 36x_4 + 49x_5 + 64x_6 + 81x_7 &= 123. \end{aligned}$$

Find the value of $16x_1 + 25x_2 + 36x_3 + 49x_4 + 64x_5 + 81x_6 + 100x_7$.

2 Exponents, Logarithms, Radicals

In this handout, we'll go over everything related to powers in algebra problems.

§2.1 Exponents & Logarithms

For an integer n, we define a^n (pronounced "a to the nth power") as $\underbrace{a \times a \times \cdots \times a}_{n}$ (where a is repeated n times). We can extend this definition to the rationals by defining $a^{1/m}$ as the mth root of a, or the number that yields a when we raise it to the power of m.

The following are some properties of exponents:

$$a^n \times a^m = a^{n+m} \tag{2.1}$$

$$a^{-n} = \frac{1}{a^n} \tag{2.2}$$

$$(a^m)^n = a^{mn} \tag{2.3}$$

Let's start with some very basic examples.

Example 2.1. What is $\frac{4^8}{4^5}$?

Solution. Using the definition at the beginning of the handout, $\frac{4\times4\times4\times4\times4\times4\times4\times4}{4\times4\times4\times4\times4} = 4^{8-5} = 4^3 = \boxed{64}$. We could also use properties 2 and 1 to get that $\frac{4^8}{4^5} = 4^8 4^{-5} = 4^{8-5} = 4^3$. ■

Example 2.2. What is $(2^2)^2$?

Solution. Using the third property, we get that $(2^2)^2 = 2^4 = 16$. Alternatively, we could just say that $(2^2)^2 = 4^2 = 16$. ■

Let's move on to the logarithm (or "log" for brevity). Here's the motivation for defining the logarithm: let's say we wanted to find x such that $2^x = 64$. How would we do this? We would need a function that "undoes" exponentiation (i.e. is the inverse of exponentiation).

In general, if $b^x = a$, then we say that $\log_b a = x$ ("log base b of a equals x"). Here are some basic properties of logs that follow from the properties of exponents.

$$\log_b 1 = 0 \tag{2.4}$$

$$\log_b x + \log_b y = \log_b xy \tag{2.5}$$

$$k \log_b x = \log_b x^k \tag{2.6}$$

$$\log_b a = \frac{\log_c a}{\log_c b} \tag{2.7}$$

Property (1.7) is known as the change of base formula, and is very useful when we want to get all our logarithms to have the same base to simplify equations. Once all our logarithms have the same base, we can repeatedly apply (1.5) and (1.6) to combine our logarithms.

Exercise 2.3. Prove properties (1.4) through (1.7) using the definition of a logarithm and exponent rules.

Exercise 2.4. Prove that $\log_{b^k} x = \frac{1}{k} \log_b x$.

Exercise 2.5. Prove that $-\log_b x = \log_b \frac{1}{x}$.

Exercise 2.6. Prove that $\log_b a = \frac{1}{\log_a b}$.

> *Remark.* We might also omit the base from a log, in which case it comes in the form $\log a$. This is usually because the base is assumed to be a number like 10.

Let's tackle some tricky problems.

Example 2.7 (2013 AIME II)**.** Positive integers a and b satisfy the condition $\log_2(\log_{2^a}(\log_{2^b}(2^{1000}))) = 0$. Find the sum of all possible values of $a + b$.

Solution. Using the properties of logarithms, we can repeatedly reduce the initial equation.

$$\begin{aligned} \log_2(\log_{2^a}(\log_{2^b}(2^{1000}))) &= 0 \\ \log_{2^a}(\log_{2^b}(2^{1000})) &= 1 \\ 2^a &= \log_{2^b}(2^{1000}) \\ (2^b)^{2^a} &= 2^{1000} \end{aligned}$$

Equating exponents, we get

$$b(2^a) = 1000.$$

Since a must be positive, and the only powers of two that divide 1000 are 2, 4, and 8, we get that our three solutions are $(a, b) = (1, 500), (2, 250), (3, 125)$. Thus, our desired sum is 881. ■

Example 2.8. If $\log_{10} 5 \approx 0.7$, how many digits are in 2^{56}?

Solution. Notice the floor of the base 10 logarithm of a number gives us one less than than the number of digits it has, since $\log_{10} 10^k = k$. For example $1 < \log_{10} 400 < 2$ and $3 < \log_{10} 2000 < 4$. Taking the base 10 logarithm of 2^{56} gives us $\log_{10} 2^{56} = 56 \log_{10} 2$. Notice that

$$\log_{10} 2 = \log_{10} 10 - \log_{10} 5 \approx 0.3.$$

Since $56(0.3) = 16.8$, it follows that 2^{56} has 17 digits. ■

Example 2.9 (2019 AMC 12A)**.** Positive real numbers a and b have the property that

$$\sqrt{\log a} + \sqrt{\log b} + \log \sqrt{a} + \log \sqrt{b} = 100$$

and all four terms on the left are positive integers, where log denotes the base-10 logarithm. What is ab?

Solution. Since we are given that the base of each logarithm is 10, it makes sense to substitute $x = \log_{10} a$, $y = \log_{10} b$. With this substitution, our equation now becomes

$$\sqrt{x} + \sqrt{y} + \frac{x}{2} + \frac{y}{2} = 100.$$

Since we know that all terms must be integers, we test even perfect squares for the values of x, y. After some plugging and chugging, we find that $(x, y) = (100, 64)$ is a solution. Thus our desired product $ab = 10^{100} \cdot 10^{64} = 10^{164}$. ■

Example 2.10 (2005 AIME I). The equation $2^{333x-2} + 2^{111x+2} = 2^{222x+1} + 1$ has three real roots. Find their sum.

Solution. Notice that the exponents all have some multiple of $111x$; thus, it makes sense to substitute $y = 2^{111x}$ to get a polynomial in y. Solving for x in terms of y, we have that $x = \frac{\log_2 y}{111}$. If our three roots are x_1, x_2, x_3, then our desired sum is

$$x_1 + x_2 + x_3 = \frac{\log_2 y_1 y_2 y_3}{111}.$$

With the substitution, our equation now becomes $\frac{y^3}{4} + 4y = 2y^2 + 1$. Multiplying by 4 and rearranging, we have that $y^3 - 8y^2 + 16y - 4 = 0$. By Vieta's, $y_1 y_2 y_3 = 4$, so our desired sum is $\frac{2}{111}$. ■

Example 2.11 (1984 AIME). Determine the value of ab if $\log_8 a + \log_4 b^2 = 5$ and $\log_8 b + \log_4 a^2 = 7$.

Solution. Subtracting the first equation from the second, we have that $\log_4 \left(\frac{a}{b}\right)^2 + \log_8 \frac{b}{a} = 2$. Since the bases aren't the same, we are motivated to change them so we can combine the logs by multiplying their arguments. Rewriting the equation and repeatedly simplifying, we get that

$$\begin{aligned} \frac{\log_2 \left(\frac{a}{b}\right)^2}{\log_2 4} + \frac{\log_2 \frac{a}{b}}{\log_2 8} &= 2 \\ \log_2 \frac{a}{b} - \frac{\log_2 \frac{a}{b}}{3} &= 2 \\ \log_2 \frac{a}{b} &= 3 \\ \frac{a}{b} &= 8. \end{aligned}$$

In our simplification, we used the fact that $\log_a b^c = c \log_a b$ and $\log_a b = -\log_a \frac{1}{b}$. Substituting $a = 8b$ back into the first equation, we have that $\log_8 8b + \log_4 b^2 = 5$. Rewriting, we get that

$$\begin{aligned} \frac{\log_2 8b}{3} + \frac{\log_2 b^2}{2} &= 5 \\ 2\log_2 8b + 3\log_2 b^2 &= 30 \\ \log_2 (64b^2)(b^6) &= 30 \\ 64b^8 &= 2^{30} \\ b &= 8. \end{aligned}$$

Thus $a = 64$ and our desired product $ab = 512$. ■

The main idea in this problem was noticing that the bases of each logarithm were powers of two. Then, we used change of base to simplify the equations and the problem was much more straightforward from there. In general, given an equation with logarithms, the first thing you should try to do is make all the bases the same, if possible.

Example 2.12 (2010 AIME II). Positive numbers x, y, z satisfy $xyz = 10^{81}$ and $(\log_{10} x)(\log_{10} yz)+(\log_{10} y)(\log_{10} z) = 468$. Find $\sqrt{(\log_{10} x)^2 + (\log_{10} y)^2 + (\log_{10} z)^2}$.

Solution. Since we are dealing with a lot of base 10 logarithms, it makes sense to make the substitution $a = \log_{10} x$, $b = \log_{10} y$, and $c = \log_{10} z$. Thus, we wish to find $\sqrt{a^2 + b^2 + c^2}$. Taking both sides $\log_{10}$ in the equation $xyz = 10^{81}$ gives us

$$\log_{10} xyz = 81 \implies a + b + c = 81.$$

We also have that

$$a(b + c) + (bc) = 468 \implies ab + bc + ac = 468$$

from the second equation. Now, we can square both sides of $a+b+c = 81$ to get $a^2+b^2+c^2+2ab+2bc+2ac = 6561$. Subtracting $2(ab + bc + ac) = 2(468)$, we get that $a^2 + b^2 + c^2 = 5625$. (Remember when we said this manipulation comes up a lot in algebra problems?) Taking the square root of both sides gives us our desired answer of 75. ■

In this problem, the key strategy was to make some clever substitutions with the given equations, allowing us to notice the needed algebraic manipulation much more quickly.

Example 2.13 (HMMT 2020 February). Let $a = 256$. Find the unique real number $x > a^2$ such that

$$\log_a \log_a \log_a x = \log_{a^2} \log_{a^2} \log_{a^2} x$$

Solution. Although we are given that $a = 256$, let's not substitute it in for the moment. Notice that all the logarithms have bases with powers of a; this is a clear sign that we should use change of base. Let's change the outermost logarithm on the RHS to base a. Our equation becomes

$$\log_a \log_a \log_a x = \frac{\log_a \log_{a^2} \log_{a^2} x}{\log_a a^2}.$$

Since $\log_a a^2 = 2$, we can simplify further:

$$2 \log_a \log_a \log_a x = \log_a \log_{a^2} \log_{a^2} x$$
$$\log_a (\log_a \log_a x)^2 = \log_a \log_{a^2} \log_{a^2} x$$

Since both sides share the same base, their arguments must be equal, so we can further simplify the equation to

$$(\log_a \log_a x)^2 = \log_{a^2} \log_{a^2} x.$$

Now, we can make the substitution $m = \log_a x$. From change of base, we find that $\frac{m}{2} = \log_{a^2} x$. Now we can reduce our equation to $(\log_a m)^2 = \log_{a^2} \frac{m}{2}$.

Using change of base on the RHS, we find that $\frac{\log_a \frac{m}{2}}{2} = \log_{a^2} \frac{m}{2}$. Thus, our equation becomes

$$2(\log_a m)^2 = \log_a \frac{m}{2}.$$

We have a square of $\log_a m$ on the LHS; this means we probably want to turn this equation into a quadratic in terms of either $\log_a m$ or $\log_a \frac{m}{2}$. Let's try the second option.

Notice that we can write $\log_a m = \log_a \frac{m}{2} + \log_a 2$. Since $a = 256 = 2^8$, we have that $\log_a 2$ is just a constant; we can write it as $\log_a m = \log_a \frac{m}{2} + \frac{1}{8}$. We now have a quadratic in terms of $\log_a \frac{m}{2}$:

$$2(\log_a \frac{m}{2} + \frac{1}{8})^2 = \log_a \frac{m}{2}.$$

This factors into $(8(\log_a \frac{m}{2})^2 - 1) = 0$. Thus, $\log_a \frac{m}{2} = \frac{1}{8} \implies \frac{m}{2} = 2 \implies m = 4$. Substituting m back into $m = \log_a x = \log_{256} x$, we have that $x = 256^4 = 2^{32}$. ■

That was a tough problem, and we had to use a lot of substitutions and base changes to solve it. Many log problems will look similarly intimidating, but they can all be simplified and eventually solved through substitutions and manipulations.

Hopefully you have a better feel for logarithm and exponent problems now; problems will usually boil down to having the intuition for what to do next (e.g. getting all the terms to have the same base or substituting variables in for logarithm terms that are used repeatedly) and knowing which logarithm properties to use to accomplish it.

Exercise 2.14 (AHSME). If $60^a = 3$ and $60^b = 5$, find $12^{[}(1 - a - b)/(2 - 2b)]$

Exercise 2.15 (CMC). Let a and b be positive real numbers satisfying

$$(\log_2 a)(\log_4 b) + a^2 = 135 \quad \text{and} \quad (\log_4 a)(\log_2 b) + b^2 = 263.$$

Then the value of ab can be written as $p\sqrt{q}$ for positive integers p and q such that q is not divisible by the square of any prime. What is $p + q$?

§2.2 Radicals

In the previous section, we discussed exponents in general. Here, we'll discuss fractional exponents, paying special attention to square roots. Roots have a tendency to show up on algebra problems that are more number-theoretic, and often require a specific kind of manipulation to deal with.

We know how to find squares of numbers very easily. For example, to find the square of 41, multiply: $41 * 41 = 1681$. However, the operation can be reversed. What number, when multiplied by itself, yields 1681? This is a lot less trivial than the previous problem because our methods are much more inefficient; we usually resort to guessing and checking or using a calculator.

> *Remark.* There actually are algorithms to find the square root of any number by hand, precise for as many digits as we want (usually numerical methods derived from calculus). However, they are still too slow to justify using over efficient guessing and checking when it comes to math competitions.

Finding a number x that multiplies by itself to produce a given number n is equivalent to looking for the **square root** of n, which is x. In notation form, the radical is used, as shown.

$$\sqrt{144} = 12$$

Here, the radical symbol above the 144 means that the square root of 144 is equal to 12.

You may start to wonder why -12 isn't a solution. Doesn't $(-12)(-12) = 144$, making -12 a possible answer? While the negative version does multiply to give the same result, radicals and square roots are defined as functions that produce only nonnegative values. You will never see a square root of a number yield a negative number. The nonnegative square root is known as the **principal square rootprincipal square root** of a number. Unless otherwise stated, when the square root symbol is used, we refer to the principal square root. Observe below:

Example 2.16. What solution(s) exist for the equation $x^2 = 400$?

Solution. Plugging in values or factoring using difference of squares, we find that $x = 20$ and $x = -20$ both work as solutions. ■

Compare the above problem with this next one:

Example 2.17. What solution(s) exist for the equation $x = \sqrt{400}$?

Solution. This seems to be the same problem as before. $x = 20$ works as a solution. However, due to the nature of principal square roots, they never output negative values. Thus, 20 is our only answer. ■

Of course, there is a reverse operation for finding the cube of a number, fourth power of a number, and so on. For example, if you want to write the "4th root of 81", you can write

$$\sqrt[4]{81} = 3$$

Note that if you wish to take an odd root of a negative number, you can expect to get a negative number back. For example, $\sqrt[5]{-32} = -2$. The idea of a principal root applies only to even powers.

As we stated before, radicals are essentially exponents. Taking the square root of a number is equivalent to raising it to the power of $\frac{1}{2}$. In general, taking the nth root of any number is equivalent to raising the number to the $\frac{1}{n}$-th power. This can help simplify expressions:

Example 2.18. The quantity $\sqrt[7]{16}$ can be expressed as 2^n for some n. What is n?

Solution. We should first notice that 16 is equal to 2^4. Also, as discussed before, taking the 7th root is equivalent to raising the number to the $\frac{1}{7}$-th power. Using exponent rules, this is equivalent to

$$(2^4)^{\frac{1}{7}} = 2^{\frac{4}{7}}$$

Thus, $n = \frac{4}{7}$. ■

Simplifying square roots are also essential in math contests, given that your answer can only be correct if expressed in simplest form. Note that

$$\sqrt{180} = 2\sqrt{45} = 3\sqrt{20} = 6\sqrt{5}.$$

Thus, if you get $\sqrt{180}$, you have to simplify it. This process is outlined below:

1. Determine a perfect square (greater than 1) that divides into the radicand (the number under the radical). Usually start with 4 and work your way up.
2. Divide the radicand by your chosen perfect square and replace your old radicand with this new quotient. Also, put the square root of your perfect square outside of the radicand.
3. Repeat steps 1 and 2 until you cannot locate any more perfect squares. At this point, you finished.

Let us demonstrate this process:

Example 2.19. Simplify $\sqrt{240}$.

Solution. Using the process outlined above, we'll try to determine perfect squares that divide into 240. Let's start with 4. Since 240 is indeed divisible by 4, we now follow step 2 and replace 240 with $\frac{240}{4} = 60$ while putting $\sqrt{4} = 2$ on the outside, getting the more simplified $2\sqrt{60}$. However, this isn't the answer because 4 yet again divides into the radicand, 60. Thus, we follow step 2 again and replace 60 with $\frac{60}{4} = 15$ and the number outside the radical, 2, with itself times $\sqrt{4} = 2$, giving us the even more simplified radical $4\sqrt{15}$. Noting that no more perfect squares divide into the new radicand 15, our answer stays as $4\sqrt{15}$. ■

Exercise. Simplify $\sqrt{735}$.

We can extend this process to nth roots as well. For example, $\sqrt[4]{324} = \sqrt[4]{4 \cdot 3^4} = 3\sqrt[4]{4}$.

Example 2.20 (Adapted from 2020 MATHCOUNTS State). A sequence is defined by $S_n = \dfrac{n(n+1)}{2}$ for all positive integers n. Another sequence is defined as $P_n = 2S_n * 2S_{n+1} * 2S_{n+2} * ... * 2S_{2n-1}$ for all positive integers n. The value of $\sqrt{P_{2019}}$ can be written in simplest radical form as $a\sqrt{b}$, where a and b are positive integers. What is the value of b?

Solution. Note that

$$2S_k = k(k+1)$$

This means that we can simplify the expression of P_n:

$$P_n = n(n+1) * (n+1)(n+2) * (n+2)(n+3) * ... * (2n-1)(2n)$$

$$P_n = n(n+1)^2(n+2)^2...(2n-1)^2 * 2n$$

Now we should derive a formula for $\sqrt{P_n}$ rather than P_n. Note that all the squared terms can be taken out of the radical as shown:

$$\sqrt{P_n} = \sqrt{n(n+1)^2(n+2)^2...(2n-1)^2 * 2n} = (n+1)(n+2)...(2n-1)\sqrt{2n^2}$$

$$= n(n+1)(n+2)...(2n-1)\sqrt{2}$$

The problem only asks for the value of b, the value inside the radicand. Clearly, no matter what n is, the value of b will always stay the same: 2. ■

§2.2.1 Conjugates

If we have an expression involving square roots, the **conjugate** is an expression we can multiply the original expression by to eliminate all square roots. For a binomial expresson $x+y$, the conjugate is $x-y$ as the difference of squares identity will usually resolve any square roots. For example, if a, b, and c are integers, the conjugate of $a+b\sqrt{c}$ is $a-b\sqrt{c}$, and the conjugate of $\sqrt{a}+\sqrt{b}$ is $\sqrt{a}-\sqrt{b}$. Conjugates are very useful for simplifying expressions involving radicals. For example, if we have a fraction with a radical in the denominator, like

$$\frac{3}{1+2\sqrt{5}},$$

then we can make the denominator rational by multiplying the top and bottom by the conjugate of the denominator:

$$\frac{3\cdot(1-2\sqrt{5})}{(1+2\sqrt{5})(1-2\sqrt{5})}=\frac{-3+6\sqrt{5}}{19}$$

Conjugates also appear very often when we have to deal with nasty radical expressions. Let's try a few examples:

Example 2.21 (2011 AMC 10A). Which of the following is equal to $\sqrt{9-6\sqrt{2}}+\sqrt{9+6\sqrt{2}}$?

(A) $3\sqrt{2}$ (B) $2\sqrt{6}$ (C) $\frac{7\sqrt{2}}{2}$ (D) $3\sqrt{3}$ (E) 6

Solution. Note that the expressions in the square roots are conjugates of each other. How can we make use of this fact? If we let $x=\sqrt{9-6\sqrt{2}}$ and $y=\sqrt{9+6\sqrt{2}}$, we know that x^2+y^2 will be an integer since the square root terms will cancel. We also know x^2y^2 is an integer.

In fact, $x^2y^2=81-72=9$ is a perfect square, so xy is also an integer. Then notice if we square the entire expression to get $x^2+2xy+y^2$, we will end up with an integer value, which will give us a simplified form of the expression when we take the square root again! So, computing $(x+y)^2$, we get

$$(x+y)^2=x^2+2xy+y^2=9-6\sqrt{2}+2\sqrt{(9-6\sqrt{2})(9+6\sqrt{2})}+9+6\sqrt{2}=18+2(3)=25.$$

Thus, $x+y=\sqrt{24}=2\sqrt{6}$ is our answer. ■

Example 2.22 (2018 AMC 10A). Suppose that real number x satisfies

$$\sqrt{49-x^2}-\sqrt{25-x^2}=3$$

What is the value of $\sqrt{49-x^2}+\sqrt{25-x^2}$?

Solution. We have a pretty messy square root expression here. Since it is in the form $\sqrt{a}-\sqrt{b}$, we should try multiplying by its conjugate to see if we get anything nice. The conjugate is of the form $\sqrt{a}+\sqrt{b}$, so we can multiply as follows:

$$(\sqrt{49-x^2}+\sqrt{25-x^2})(\sqrt{49-x^2}-\sqrt{25-x^2})=49-x^2-25+x^2=24$$

That worked nicely. We are given that

$$\sqrt{49-x^2}-\sqrt{25-x^2}=3$$

so

$$\sqrt{49-x^2}+\sqrt{25-x^2}=\frac{24}{3}=8.$$

■

Though conjugation is useful for square roots, we often have to rationalize denominators with expressions containing cube roots as well. In these cases, the difference/sum of cubes identities can be very helpful:

$$a^3+b^3=(a+b)(a^2-ab+b^2)$$

and

$$a^3-b^3=(a-b)(a^2+ab+b^2)$$

Example 2.23 (2013 AIME I)**.** The real root of the equation $8x^3-3x^2-3x-1=0$ can be written in the form $\frac{\sqrt[3]{a}+\sqrt[3]{b}+1}{c}$, where a, b, and c are positive integers. Find $a+b+c$.

Solution. Looking at the last three terms of the LHS of the equation reminds us of the expansion $(x+1)^3$. So it seems like a good idea to rewrite

$$8x^3-3x^2-3x-1=9x^3-(x+1)^3=0$$

Now we can solve this equation quite easily:

$$9x^3-(x+1)^3=0 \implies 9x^3=(x+1)^3 \implies \sqrt[3]{9}x=x+1$$

since real cube roots are unique. This gives us $x=\frac{1}{\sqrt[3]{9}-1}$. But to get this in the desired form, we have to rationalize the denominator. This is where the difference of cubes identity comes in: we know that

$$(\sqrt[3]{9}-1)(\sqrt[3]{81}+\sqrt[3]{9}+1)=9-1=8.$$

Then

$$\sqrt[3]{9}-1=\frac{8}{\sqrt[3]{81}+\sqrt[3]{9}+1},$$

so

$$x=\frac{\sqrt[3]{81}+\sqrt[3]{9}+1}{8}.$$

Thus, our answer is $81+9+8=98$. ■

Conjugates serve as an important tool for eliminating roots. More generally, its important to remember algebraic identities like difference of cubes and difference of squares, as these are essential to eliminating roots and rationalizing expressions, greatly simplifying problems.

Exercise 2.24. Rationalize the denominator of $\frac{5}{\sqrt[3]{7}+1}$.

Exercise 2.25. Rationalize the denominator of $\frac{6}{\sqrt[4]{3}+\sqrt[4]{2}}$.

§2.3 Homework Problems

Problem 2.1 (2010 AMC 12A)**.** [4] The solution of the equation $7^{x+7} = 8^x$ can be expressed in the form $x = \log_b 7^7$. We can write b as a fraction $\frac{p}{q}$ in simplest form, where p and q are integers. What is $p + q$?

Problem 2.2 (1984 AIME)**.** [4] Determine the value of ab if $\log_8 a + \log_4 b^2 = 5$ and $\log_8 b + \log_4 a^2 = 7$.

Problem 2.3 (2013 AMC 12A)**.** [4] The sequence $\log_{12} 162$, $\log_{12} x$, $\log_{12} y$, $\log_{12} z$, $\log_{12} 1250$ is an arithmetic progression. What is x?

Problem 2.4 (2008 AMC 12B)**.** [4] A circle has a radius of $\log_{10}(a^2)$ and a circumference of $\log_{10}(b^4)$. What is $(\log_a b)/\pi$?

Problem 2.5 (2000 AIME I)**.** [6] The system of equations

$$\begin{aligned} \log_{10}(2000xy) - (\log_{10} x)(\log_{10} y) &= 4 \\ \log_{10}(2yz) - (\log_{10} y)(\log_{10} z) &= 1 \\ \log_{10}(zx) - (\log_{10} z)(\log_{10} x) &= 0 \end{aligned}$$

has two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2). Find $y_1 + y_2$.

Problem 2.6 (2008 AMC 12B)**.** [7] The sum of the base-10 logarithms of the divisors of 10^n is 792. What is n?

Problem 2.7 (2006 AIME I)**.** [8] The number $\sqrt{104\sqrt{6} + 468\sqrt{10} + 144\sqrt{15} + 2006}$ can be written as $a\sqrt{2} + b\sqrt{3} + c\sqrt{5}$, where a, b, and c are positive integers. Find abc.

Problem 2.8 (2019 AMC 12A)**.** [10] Define binary operations $\diamondsuit$ and $\heartsuit$ by

$$a \diamondsuit b = a^{\log_7(b)} \qquad \text{and} \qquad a \heartsuit b = a^{\frac{1}{\log_7(b)}}$$

for all real numbers a and b for which these expressions are defined. The sequence (a_n) is defined recursively by $a_3 = 3 \heartsuit 2$ and

$$a_n = (n \heartsuit (n-1)) \diamondsuit a_{n-1}$$

for all integers $n \geq 4$. To the nearest integer, what is $\log_7(a_{2019})$?

Problem 2.9 (2019 AIME I)**.** [10] There are positive integers x and y that satisfy the system of equations

$$\log_{10} x + 2\log_{10}(\gcd(x, y)) = 60$$
$$\log_{10} y + 2\log_{10}(\operatorname{lcm}(x, y)) = 570.$$

Let m be the number of (not necessarily distinct) prime factors in the prime factorization of x, and let n be the number of (not necessarily distinct) prime factors in the prime factorization of y. Find $3m + 2n$.

Problem 2.10 (2018 AIME I)**.** [7] For each ordered pair of real numbers (x, y) satisfying

$$\log_2(2x + y) = \log_4(x^2 + xy + 7y^2)$$

there is a real number K such that

$$\log_3(3x + y) = \log_9(3x^2 + 4xy + Ky^2).$$

Find the product of all possible values of K. **Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.**

3 Sequences and Series

Sequences and series are **everywhere** on the AMC 10/12 and AIME — this is no exaggeration. This handout will cover the various types of sequences and series you are likely to encounter.

§3.1 Arithmetic and Geometric Sequences and Series

Before we get into series, we'll define arithmetic and geometric sequences.

Definition 3.1. A **arithmetic** sequence is a sequence a_n where consecutive terms differ by a constant value, known as the common difference. For example, $a_n = 2n + 3$ is an arithmetic sequence with $a_0 = 3$ and common difference 2.

Definition 3.2. A **geometric** sequence is a sequence g_n where consecutive terms have a constant ratio, known as the common ratio. For example, $g_n = 5 \cdot 3^n$ is a geometric sequence with $g_0 = 5$ and common ratio 3.

Now let's get into arithmetic series; recall that an arithmetic series is a sum of any number of consecutive terms in an arithmetic sequence.

Here's a simple example that illustrates a general process that can be used to sum arithmetic series:

Example. Sum the series $1 + 2 + 3 + \cdots + 100$.

Solution. The solution most commonly attributed to a young Gauss proceeds as follows: pair up 1 and 100; 2 and 99; 3 and 98; and similarly pair up the rest of the terms until 50 and 51. Then each pair of terms sums to 101, and there are 50 pairs in total. (Why?) Thus it follows that the total sum is $50 \cdot 101 = 5050$. ■

Remark. Pretty much all arithmetic series can be summed using the same manner — while there is a formula, it's quite easy to just derive on the spot, so we wouldn't recommend memorizing it. Pair up terms, find how many pairs there are, and multiply!

Example. Find the sum of the series $1 + 3 + 5 + \cdots + (2n - 1)$ in terms of n.

Solution. Let's try our pairing-up method again: 1 goes with $2n - 1$; 3 goes with $2n - 3$; and so on — all looks the same as before, right?

There's one small hurdle we might run into: all our pairs have an average of n and sum to $2n$ — they're kind of "centered around n", in a way. But what if n itself is odd? Then $n - 2$ and $n + 2$ would make a pair, but n itself wouldn't have another n to pair with.

So we take cases. First, suppose that n is indeed odd. There are n terms in total in the series (why?) so there must be $\frac{n-1}{2}$ pairs, with one middle element n alone. Each pair sums to $2n$, so our total is $\frac{n-1}{2} \cdot 2n + n = n^2$. Thus the sum comes out to be n^2 if n is odd.

What if n is even? Then the two terms nearest n are $n-1$ and $n+1$, which pair up very nicely and sum to $2n$, just like 1 and $2n-1$, 3 and $2n-3$, and all the other terms. In this case, there are n terms and therefore $\frac{n}{2}$ pairs of terms, each pair summing to $2n$, so we get $\frac{n}{2} \cdot 2n = n^2$ as the sum of our series. It turns out the the sum is n^2 whether n is even or odd — how nice! ■

Before we move on, we're going to quickly introduce some helpful notation:

Definition 3.3. The symbol $\sum$ denotes a sum. Specifically, $\sum_{i=1}^{n} f(i)$, where $f(i)$ is any function of i, is just telling us to add $f(i)$ for i from 1 all the way up to n — that is, $\sum_{i=1}^{n} f(i) = f(1) + f(2) + \cdots + f(n)$.

For the first example we provided in the section, we might have

$$\sum_{i=1}^{100} i = 1 + 2 + \cdots + 100.$$

As for the second, it would be

$$\begin{aligned}\sum_{i=1}^{n}(2i-1) &= [2(1)-1] + [2(2)-1] + [2(3)-1] + \cdots + [2(n)-1] \\ &= 1 + 3 + 5 + \cdots + (2n-1).\end{aligned}$$

For a tougher example, if we wanted $1 - 4 + 9 - 16 + 25 - 36 + \cdots - 10000$, we could write this as

$$\sum_{i=1}^{100}(-1)^{i+1} i^2.$$

We've introduced the -1 power to handle the alternating nature of the sum, and the i^2 is used to generate squares. (Try to figure out why this works on your own — plug in $i = 1, 2$, and 3, and convince yourself that these are equivalent representations of the sum!)

We can also write sums to infinity: we know that $1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2$, where successive terms are generated by dividing previous terms by 2. But this can equivalently be written as

$$\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i = \left(\frac{1}{2}\right)^0 + \left(\frac{1}{2}\right)^1 + \left(\frac{1}{2}\right)^2 + \cdots = 2.$$

The variable i is called a **dummy variable** in that it doesn't actually matter in the end — $\sum_{i=1}^{100} i = \sum_{k=1}^{100} k = 1 + 2 + 3 + \cdots + 100$, for example. The most common dummy variables that we use are i, j, and k for sums.

It turns out that we can write products in much the same way, although we won't consider that in this handout: $\prod_{i=1}^{10} i = 10!$, for example.

Exercise 3.4. Derive a general formula for the sum of the series $\sum_{j=1}^{n} j = 1 + 2 + 3 + \cdots + n$. (Yes, you've probably seen this before, but give it another try!)

Now we'll move onto a somewhat harder task: summing geometric series.

Example. Derive a formula for the sum of the infinite geometric series $\sum_{i=0}^{\infty} ar^i$, with $|r| < 1$. (Here, we refer to r as the **common ratio** for the series.)

Solution. Unpacking the notation, we see that $\sum_{i=0}^{\infty} ar^i = ar^0 + ar^1 + ar^2 + \cdots$. Let's let $S = a + ar + ar^2 + ar^3 + \cdots$. We can see that

$$rS = ar + ar^2 + ar^3 + ar^4 + \cdots.$$

Great! It turns out that S and rS actually look a lot like each other. Indeed, we actually get $S = a + rS$ — there's an entire copy of rS embedded in S. Now, with this new equation $S = a + rS$, moving all the S terms to one side and dividing yields

$$S = \frac{a}{1-r}$$

and so we've derived a formula for S, the sum of the series. ■

A few things to note: there's nothing special, actually, about our a and r here. Indeed, for any starting value a and common ratio r with $|r| < 1$, it's true tha the sum $a + ar + ar^2 + \cdots = \frac{a}{1-r}$.

We haven't actually mentioned why $|r| < 1$ is necessary. Suppose that $r = 2$, and $a = 1$, for example. Then our series becomes

$$S = 1 + 2 + 4 + 8 + \cdots$$

which we might sum as $S = \frac{1}{1-2} = -1$. That doesn't look right — all the terms are positive!

Remark. An infinite geometric series is said to **diverge** if the common ratio r satisfies $|r| \geq 1$. That means that when you try to sum the series, it goes out to infinity or negative infinity — it doesn't approach some finite number. In this case, you **cannot** use the formula we've learned to sum the series.

Let's put everything together one last time.

Theorem 3.5 (Sum of Geometric Series). *The sum $\sum_{i=0}^{\infty} ar^i = a + ar + ar^2 + \cdots$ is equal to*

$$\frac{a}{1-r}$$

where a is the first term of the series, and r is the common ratio of the series.

Remark. This is just a formula for the sum of an infinite geometric series — if you have to deal with finite geometric series, the formula is a bit uglier. To that end, finite geometric series can be summed using the same method as infinite geometric series, though: let S be the sum of the finite series, multiply the entire thing by the common ratio (let's call it r), and use the fact that S and rS are super similar. For example,

$$S = 3 + 9 + 27 + \cdots + 729$$

gives us

$$3S = 9 + 27 + 81 + \cdots + 2187$$

so therefore, $S = 3 + (3S) - 2187$. From there you can find $S = 1092$.

In general, the sum of the first n terms of a geometric series is

$$\frac{a(1-r^n)}{1-r}$$

where a is the first term and r is the common ratio. Try proving this yourself, using the method we just outlined.

Exercise 3.6. Argue that $0.\overline{9} = 0.999\ldots = 1$ with Theorem 3.5.

Great! Let's move onto some harder examples, from competitions.

Example (2016 AIME I). For $-1 < r < 1$, let $S(r)$ denote the sum of the geometric series

$$12 + 12r + 12r^2 + 12r^3 + \ldots.$$

Let a between -1 and 1 satisfy $S(a)S(-a) = 2016$. Find $S(a) + S(-a)$.

Solution. We're trying to deal with the condition $S(a)S(-a) = 2016$, so our first step should probably be to address $S(a)$ and $S(-a)$. We have, by the infinite geometric series formula,

$$S(a) = 12 + 12a + 12a^2 + 12a^3 \cdots = \frac{12}{1-a}$$
$$S(-a) = 12 - 12a + 12a^2 - 12a^3 + \cdots = \frac{12}{1+a}$$

as 12 is the first term of both series, and the first series has common ratio a and the second has common ratio $-a$.

Great. So now we have

$$\frac{12}{1-a} \cdot \frac{12}{1+a} = \frac{144}{(1-a)(1+a)} = 2016.$$

One thing we'll continuously emphasize is that before rushing forward and solving equations like the above one, it's best to first check what we're looking for — that is, $S(a)+S(-a)$. Using the previously-derived formulas, we have

$$\begin{aligned} S(a) + S(-a) &= \frac{12}{1-a} + \frac{12}{1+a} \\ &= \frac{12(1+a) + 12(1-a)}{(1+a)(1-a)} \\ &= \frac{24}{(1+a)(1-a)}. \end{aligned}$$

Nice! It turns out that we already have $\frac{144}{(1-a)(1+a)} = 2016$, so all we have to do is divide by 6, giving us

$$\frac{24}{(1-a)(1+a)} = 336$$

so our answer is 336. ■

A few takeaways: remember firstly that infinite series can be summed really nicely, whether their common ratios are positive or negative! And as discussed before in Section 1.1, remember to check what you're looking for before blindly running ahead and finding the values of variables — sometimes it's easier without explicitly finding them, such as in this problem where we didn't need to actually solve for a.

Example (2012 AIME I). The terms of an arithmetic sequence add to 715. The first term of the sequence is increased by 1, the second term is increased by 3, the third term is increased by 5, and in general, the kth term is increased by the kth odd positive integer. The terms of the new sequence add to 836. Find the sum of the first, last, and middle terms of the original sequence.

Solution. We've got a bunch of words here — the first thing we should do is translate them into math. Suppose that our arithmetic sequence is $a_1, a_2, a_3, \cdots, a_n$; keep in mind that we still don't know how many terms there are! Then

$$\begin{aligned} a_1 + a_2 + a_3 + \cdots + a_n &= 715 \\ (a_1 + 1) + (a_2 + 3) + (a_3 + 5) + \cdots + (a_n + (2n-1)) &= 836 \end{aligned}$$

where we've noticed that each term of the new sequence is of the form $a_k + (2k-1)$. (Why?)

Note that in our second equation, there's actually an $a_1 + a_2 + a_3 + \cdots + a_n$ — it's just hidden! So we get

$$\begin{aligned} 836 &= (a_1 + a_2 + a_3 + \cdots + a_n) + (1 + 3 + 5 + \cdots + (2n-1)) \\ &= 715 + (1 + 3 + 5 + \cdots + (2n-1)). \end{aligned}$$

Recall from an earlier example that the sum $1 + 3 + 5 + \cdots + (2n-1)$ is just n^2. Therefore $836 = 715 + n^2$, and $n = 11$.

Now we're looking for the sum of the first, last, and middle terms of the original sequence. This means that we want to find $a_1 + a_6 + a_{11}$. Note that as $a_1, a_2, a_3, \cdots, a_{11}$ is an arithmetic sequence, it's "centered" around a_6 — that is, a_5 and a_7's average is a_6, a_4 and a_8's average is a_6, and so on. (Why? Think about the fact that if the common difference is d, the terms before and after a in a sequence are $a - d$ and $a + d$.)

So thus we know that $a_1 + a_{11} = 2a_6$; $a_2 + a_{10} = 2a_6$; and reducing all the terms this way, we find the equation

$$11a_6 = 715.$$

Meanwhile, we're just looking for $a_1 + a_6 + a_{11} = 3a_{11}$. Thus our final answer is $\frac{3}{11} \cdot 715 = 195$, and we're done. ■

Example 3.7 (2020 AMC 10). There exists a unique strictly increasing sequence of non-negative integers $a_1 < a_2 < \ldots < a_k$ such that

$$\frac{2^{289} + 1}{2^{17} + 1} = 2^{a_1} + 2^{a_2} + \ldots + 2^{a_k}.$$

What is k?

Solution. At first glance, this seems like a pretty tough problem; $2^{289} + 1$ and $2^{17} + 1$ are massive numbers and essentially impossible to prime factorize, so we can't do the brute force approach of finding $(2^{289} + 1)/(2^{17} + 1)$ then computing its binary representation. However, the idea of representing the expression as a sum of powers of 2 brings to mind geometric series. Can we find a connection? Noting that $289 = 17^2$, the expression

$$\frac{2^{17^2} + 1}{2^{17} + 1}$$

looks suspiciously like the sum of a geometric series with first term 1, if we let $r = -2^{17}$. Converting the expression to the form of the geometric series formula gives

$$\frac{1-(-2^{17})^{17}}{1-(-2^{17})} = \frac{1-r^{17}}{1-r}.$$

Then we know this is the sum of the first $17-1=16$ terms of a geometric sequence with first term 1, so this is equal to

$$1 + r + r^2 + \ldots r^{16} = 2^0 - 2^{17} + 2^{34} - \cdots + 2^{272}.$$

This isn't quite what we were looking for, since we have some negative powers of 2. How can we fix this? The simplest option seems to be adding every negative power of 2 to the positive power of 2 which follows it:

$$2^0 + (-2^{17} + 2^{34}) + (-2^{51} + 2^{68}) - \cdots + (-2^{255} + 2^{272}).$$

The reason this is promising is because every negative-positive pair differs from the next pair by a factor of 2^{34}, so the binary representations will have 1s in different positions. This means we'll get distinct powers of 2 from each pair, so we can put them in strictly increasing order just like the problem asks. Note that each pair factors as $2^{17k}(-1+2^{17})$ for some integer k. Here we can use the fact that

$$-1 + 2^n = 1 + 2 + 2^2 + \cdots + 2^{n-1}.$$

This is a pretty common trick that helps to memorize and is easy to derive using geometric series. Using this fact, each pair can be turned into a sum of powers of two:

$$2^{17k}(-1+2^17) = 2^{17k}(2^0 + 2 + 2^2 + \cdots + 2^{16}) = 2^{17k} + 2^{17k+1} + 2^{17k+2} + \cdots + 2^{17k+16}.$$

It's clear that all the powers of 2 will be distinct since pairs differ by a factor of 2^{34}. Then since there are 8 pairs with 17 powers of 2 each along with the term 2^0 at the beginning, there are a total of $17 \times 8 + 1 = 137$ powers of two. ■

It turns out that most arithmetic and geometric sequences and series problems on math competitions end up being a bit formulaic. In the next section, we'll go over some different types sequences and series — ones that aren't simply arithmetic and geometric.

Exercise 3.8 (2012 AIME II). Two geometric sequences $a_1, a_2, a_3, \ldots$ and $b_1, b_2, b_3 \ldots$ have the same common ratio, with $a_1 = 27$, $b_1 = 99$, and $a_{15} = b_{11}$. Find a_9.

§3.2 Other Sequences and Series

While arithmetic and geometric series are the most common types of sums, there are many other series problems that don't fit well in either of these two categories. One of these is a mix of the two, and it is creatively named the "arithmetico-geometric series."

Example. Compute the infinite sum $\displaystyle\sum_{i=1}^{\infty} \frac{i}{3^i} = \frac{1}{3} + \frac{2}{9} + \frac{3}{27} + \frac{4}{81} + \cdots$.

Solution. It turns out that using the S and rS trick used to derive Theorem 3.5, with $r = 3$, and then applying the same theorem directly on the resulting sum solves the problem (try it out for yourself!). However, we provide an alternate approach for the sake of variety.

Let's try to view this problem from a different perspective. Right now, the infinite sum is expressed in such a way so that we don't have a formula to arrive at an immediate answer. What if we break it down into different chunks that are easier to work with? We know, for example, how to quickly find $\frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \cdots$, which looks suspiciously similar to the problem we have at hand. If we continue down this train of thought, we get the following:

$$\begin{aligned} S = &\frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \frac{1}{81} + \cdots \\ &+ \frac{1}{9} + \frac{1}{27} + \frac{1}{81} + \cdots \\ &+ \frac{1}{27} + \frac{1}{81} + \cdots \end{aligned}$$

If we sum the expression above vertically, we obtain the expression that we originally started with. However, if we sum it horizontally using Theorem 3.5, we get $S = \frac{1}{2} + \frac{1}{6} + \frac{1}{18} + \cdots$. Applying the theorem once again gives us a final value of $\frac{3}{4}$. ■

We solved this problem by quite literally changing perspectives. This is a good strategy to use whenever you're dealing with something that looks suspiciously familiar, but not quite right — turn the problem into something that you *do* know how to work with.

Exercise 3.9. Sum the series $\displaystyle\sum_{j=1}^{\infty} \frac{2j-1}{2^j} = \frac{1}{2} + \frac{3}{4} + \frac{5}{8} + \frac{7}{16} + \cdots$.

Another common type of infinite series is the **telescoping series**, which is when a lot of the terms in the sequence cancel out rather nicely, leaving one clean expression at the end. We use the word "telescope" to describe such a series, since each next term collapses the series, similarly to how a long, retractable telescope can collapse to a size no bigger than a pencil. This description may be rather confusing, so it's best to illustrate the concept with an example:

Example. Find $\displaystyle\sum_{i=1}^{\infty} \frac{1}{i \cdot (i+1)} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots$

Solution. Note that

$$\frac{1}{n(n+1)} = \frac{n+1}{n(n+1)} - \frac{n}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

This is great, because our original problem can now be written as the following:

$$\sum_{i=1}^{\infty} \left(\frac{1}{i} - \frac{1}{i+1} \right) = \left(\frac{1}{1} - \frac{1}{2} \right) + \left(\frac{1}{2} - \frac{1}{3} \right) + \left(\frac{1}{3} - \frac{1}{4} \right) + \left(\frac{1}{4} - \frac{1}{5} \right) \cdots$$

As you can see, each next term collapses on itself, leaving a rather nice looking sum! Taking this expression as it approaches infinity, it's easy to see that the sum itself approaches 1. ■

Let's take a look at the motivation behind this problem — we mentioned before that in general, telescoping sums collapse after each term. To see what this means, let's let $S_n = \sum_{i=1}^{n} \frac{1}{i \cdot (i+1)}$.

Trying out a few values by hand, we see that $S_1 = \frac{1}{2}$, $S_2 = \frac{2}{3}$, and $S_3 = \frac{3}{4}$. From here, it's reasonable to conclude that $S_k = 1 - \frac{1}{k+1}$, but can we prove why this must be the case?

We've calculated already that $S_1 = 1 - \frac{1}{2}, S_2 = 1 - \frac{1}{3}$, and $S_3 = 1 - \frac{1}{4}$. These S_n's have another nice property in general, though: they share a lot of common terms. That is, if we have S_{n-1} and S_n, all their terms up to the last $\frac{1}{n\cdot(n+1)}$ will be the same. When we have a situation like this it's often nice to subtract S_{n-1} from S_n, then — recall our proof of the geometric series formula, in which we ended up with a bunch of common terms and subtracted.

So $S_n - S_{n-1} = \frac{1}{n\cdot(n+1)}$, from definition. But now let's look back at our smaller cases: $S_2 - S_1 = \frac{1}{2} - \frac{1}{3}$; $S_3 - S_2 = \frac{1}{3} - \frac{1}{4}$. Miraculously enough, our equation at the beginning of this paragraph yields $S_2 - S_1 = \frac{1}{2\cdot3}$, and $S_3 - S_2 = \frac{1}{3\cdot4}$. At this point, the pattern that $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$ should be quite visible — and we can proceed as in the solution.

> *Remark.* Sometimes, it's not easy to determine how exactly a series $\sum a_i$ telescopes. If you ever get stuck, try to relate each a_i to a different sequence, b_i, such that $a_i = b_{i+1} - b_i$. In this particular example, $a_i = \frac{1}{i\cdot(i+1)}$ and $b_i = -\frac{1}{i}$. With this in mind, the sum of the first n terms of the sequence of a_i's will simply evaluate to $b_{n+1} - b_1$.

Let's look at a harder example; here, the telescoping substitution will be trickier to spot.

> **Example** (2018 Math Prize for Girls)**.** Consider the sum
>
> $$S_n = \sum_{k=1}^{n} \frac{1}{\sqrt{2k-1}}\,.$$
>
> Determine $\lfloor S_{4901} \rfloor$. Recall that $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

Solution. Accurately summing square roots is next to impossible, so let's see if we can bound the expression at hand in between two values. This usually requires a telescoping approach, so we'll go with that route here. To account for edge cases that will arise later, let's define

$$T_n = \sum_{k=2}^{n} \frac{1}{\sqrt{2k-1}}$$

so that $1 + T_n = S_n$. Now, notice that

$$\sqrt{2k-1} + \sqrt{2(k-1)-1} < 2\sqrt{2k-1} < \sqrt{2(k+1)-1} + \sqrt{2k-1}.$$

Taking the reciprocals and rationalizing the denominators will leave us with

$$\frac{\sqrt{2k-1} - \sqrt{2(k-1)-1}}{2} > \frac{1}{2\sqrt{2k-1}} > \frac{\sqrt{2(k+1)-1} - \sqrt{2k-1}}{2}.$$

So in reality, we have that

$$\sum_{k=2}^{n} \left(\sqrt{2(k+1)-1} - \sqrt{2k-1}\right) < T_n < \sum_{k=2}^{n} \left(\sqrt{2k-1} - \sqrt{2(k-1)-1}\right).$$

This sum telescopes — if we set $n = 4901$, we see that a lot of the summands in both the lower and upper bounds of the inequalities cancel, leaving us with just

$$\sqrt{9803} - \sqrt{3} < T_{4901} < \sqrt{9801} - \sqrt{1}$$

The upper bound is exactly 98, and, using crude estimates of $\sqrt{3} \approx 1.71$ and $\sqrt{9803} \approx 99$, the lower bound is a little bit more than 97. Thus, $\lfloor T_{4901} \rfloor = 97$, and so $\lfloor S_{4901} \rfloor = 98$. ■

The main idea behind solving this problem is bounding this sum between two easier-to-find integers, as we're only asked to find the floor of this sum. To do so, we'll probably want the lower and upper bounds to be in the form of a telescoping series involving square roots. Referring back to the remark made after the previous problem, our telescoping series should most likely be one whose summands are in the form $\sqrt{n+2} - \sqrt{n}$, as we're only summing the reciprocals of the square roots of every other number in our original expression. It turns out that these key insights are all that we needed, and the rest of the solution comes quite naturally!

§3.3 Bashing Sequences

There are some functions that just *feel* bashable. You'll know which these are through intuition and experience. They're either repeating, or their pattern becomes clear after you compute three or four terms. All you have to do is plow through.

One type of sequence problems should be bashed directly with the numbers given; the other type should be bashed in terms of variables. The key (and often only) observation is figuring out which is which.

Example 3.10 (2019 AMC 10A). A sequence of numbers is defined recursively by $a_1 = 1$, $a_2 = \frac{3}{7}$, and

$$a_n = \frac{a_{n-2} \cdot a_{n-1}}{2a_{n-2} - a_{n-1}}$$

for all $n \geq 3$. Then a_{2019} can be written as $\frac{p}{q}$, where p and q are relatively prime positive integers. What is $p + q$?

Solution. We calculate a few terms to get a feel for the problem. Note that $a_3 = \frac{3}{11}$, $a_4 = \frac{3}{15}$, and $a_5 = \frac{3}{19}$. This leads us to believe $a_n = \frac{3}{4n-1}$, and checking that this holds for a_1 is enough to convince us that $a_{2019} = \frac{3}{4 \cdot 2019 - 1} = \frac{3}{8075}$, so the answer is 8078.

In fact we can verify with induction that $a_n = \frac{3}{4n-1}$. The base case a_1 is already done, and

$$a_{n+1} = \frac{a_{n-1} \cdot a_n}{2a_{n-1} - a_n} = \frac{\frac{3}{4n-1} \cdot \frac{3}{4n-5}}{2 \cdot \frac{3}{4n-5} - \frac{3}{4n-1}} = \frac{9}{12n+9} = \frac{3}{4n+3}$$

finishes the inductive step. ■

This is a problem where you bash directly with the given numbers, because you feel the given numbers might be special in some way.

The next example contains a periodic sequence. We say a sequence is **periodic** if its terms eventually repeat. The **period** of a periodic sequence is the minimum number of terms before each repeat. For example, $1, 2, 3, 1, 2, 3, \ldots$ is periodic, and has period 3. The sequence $1, 5, 2, 4, 8, 1, 2, 3, 1, 2, 3, \ldots$ is periodic as well, because it eventually repeats forever, even though the first few terms did not repeat.

Exercise. Assume we have a sequence a_n such that each term depends only on the previous two terms. Show that if $a_{100} = a_{102}$ and $a_{101} = a_{103}$, then the sequence is periodic. In general, if we have a sequence where each successive term depends on the previous k terms, how many terms need to repeat before we can confirm the sequence is periodic?

Example 3.11 (2020 AIME II). Define a sequence recursively by $t_1 = 20$, $t_2 = 21$, and

$$t_n = \frac{5t_{n-1} + 1}{25t_{n-2}}$$

for all $n \geq 3$. Then t_{2020} can be written as $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p + q$.

Solution. Playing with this sequence for a little bit doesn't reveal much about it, so we might assume there's a pattern we have to bash to find. We'll write everything in terms of t_1 and t_2. Note

$$t_3 = \frac{5t_2 + 1}{25t_1}$$

$$t_4 = \frac{5 \cdot \frac{5t_2+1}{25t_1} + 1}{25t_2} = \frac{5t_1 + 5t_2 + 1}{125t_1t_2}$$

$$t_5 = \frac{5 \cdot \frac{5t_1+5t_2+1}{125t_1t_2} + 1}{25 \cdot \frac{5t_2+1}{25t_1}} = \frac{5t_1 + 5t_2 + 1 + 25t_1t_2}{125t_2^2 + 25t_2} = \frac{(5t_1 + 1)(5t_2 + 1)}{25t_2(5t_2 + 1)} = \frac{5t_1 + 1}{25t_2}$$

$$t_6 = \frac{5 \cdot \frac{5t_1+1}{25t_2} + 1}{25 \cdot \frac{5t_1+5t_2+1}{125t_1t_2}} = \frac{5t_1^2 + 5t_1t_2 + t_1}{5t_1 + 5t_2 + 1} = t_1.$$

So we see that this sequence repeats with a period of 5. Thus $t_{2020} = t_5 = \frac{5 \cdot 20 + 1}{5 \cdot 21} = \frac{101}{125}$, so the answer is 226. ■

This is a problem where you bash with the given variables because you feel that the recursion should have some fixed period *no matter the starting values*.

§3.4 Problems

Problem 3.1 (2015 AMC 8)**.** [4] An arithmetic sequence is a sequence in which each term after the first is obtained by adding a constant to the previous term. For example, $2, 5, 8, 11, 14$ is an arithmetic sequence with five terms, in which the first term is 2 and the constant added is 3. Each row and each column in this 5×5 array is an arithmetic sequence with five terms. What is the value of X?

1				25
		X		
17				81

Problem 3.2 (1969 AHSME)**.** Let S_n and T_n be the respective sums of the first n terms of two arithmetic series. If $S_n : T_n = (7n + 1) : (4n + 27)$ for all n, the ratio of the eleventh term of the first series to the eleventh term of the second series can be expressed as $a : b$ where a and b are relatively prime positive integers. What is $a + b$?

Problem 3.3 (2016 AMC 10B)**.** [6] The sum of an infinite geometric series is a positive number S, and the second term in the series is 1. What is the smallest possible value of S?

Problem 3.4 (2011 AIME II)**.** [6] The sum of the first 2011 terms of a geometric sequence is 200. The sum of the first 4022 terms is 380. Find the sum of the first 6033 terms.

Problem 3.5 (2002 AMC 12A)**.** [7] Consider the sequence of numbers: $4, 7, 1, 8, 9, 7, 6, \ldots$ For $n > 2$, the n-th term of the sequence is the units digit of the sum of the two previous terms. Let S_n denote the sum of the first n terms of this sequence. What is the smallest value of n for which $S_n > 10,000$?

Problem 3.6 (2002 AIME II)**.** [7] Two distinct, real, infinite geometric series each have a sum of 1 and have the same second term. The third term of one of the series is $1/8$, and the second term of both series can be written in the form $\frac{\sqrt{m}-n}{p}$, where m, n, and p are positive integers and m is not divisible by the square of any prime. Find $100m + 10n + p$.

Problem 3.7 (1989 AIME)**.** [7] If the integer k is added to each of the numbers 36, 300, and 596, one obtains the squares of three consecutive terms of an arithmetic series. Find k.

Problem 3.8 (2001 AMC 12)**.** [8] Consider sequences of positive real numbers of the form $x, 2000, y, \ldots$ in which every term after the first is 1 less than the product of its two immediate neighbors. For how many different values of x does the term 2001 appear somewhere in the sequence?

Problem 3.9 (USAMTS)**.** [10] Let

$$A = \sqrt{1 + \frac{1}{1^2} + \frac{1}{2^2}} + \sqrt{1 + \frac{1}{2^2} + \frac{1}{3^2}} + \cdots + \sqrt{1 + \frac{1}{2019^2} + \frac{1}{2020^2}}.$$

Then we can write $A/2019$ as a fraction $\frac{p}{q}$, where p and q are integers, in lowest terms. Find $p + q$.

Problem 3.10 (2005 AIME II)**.** [8] An infinite geometric series has sum 2005. A new series, obtained by squaring each term of the original series, has 10 times the sum of the original series. What is the common ratio of the original series?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

4 Polynomials

§4.1 General form

Polynomials appear very often in math competitions, and are a major topic in algebra. Let's start with the definition of a polynomial:

Definition 4.1. For constants $a_0, a_1, \ldots a_n$, $a_n \neq 0$, and nonnegative integer n, the expression

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n$$

is a **polynomial**.

Example 4.2. Which of the following are polynomials?

1. 5
2. $\frac{1}{x} + x^7 + 3$
3. $x^{-2} + x^2$
4. $x^2 + 124$
5. $x^3 + 3x + \sqrt{2}$
6. $\frac{123456789}{x^{12}} + 13$
7. $x^{\frac{2}{3}} + 6x$

Solution. What makes something not a polynomial? The condition that strikes the eye is the nonnegative integer part. For an expression to be a polynomial, all of the exponents of the x terms must be 0 or greater. So all the expressions except 3, 6, and 7 are polynomials.

■

Now we'll define some important terms we use to describe a polynomial. As we said before, we can express a polynomial as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n$$

for nonnegative integer n and constants $a_0, a_1, \ldots a_n$ with a_n nonzero.

The **degree** of a polynomial is n, the highest power of x that appears in the polynomial. A **coefficient** is any of the $a_0, a_1, \ldots a_n$, and we call a_n the **leading coefficient** of $f(x)$. A **root** of $f(x)$ is some constant r such that $f(r) = 0$.

An **integer polynomial** is a polynomial where all the coefficients are integers, and this can be similarly defined for polynomials with coefficients that are rational, real, etc.

Constants denote polynomials of degree 0, **linear** terms denote polynomials of degree 1 (e.g. $3x + 4$), **quadratic** terms denote polynomials of degree 2 (e.g. $3x^2 + 2x + 5$), **cubic** terms denote polynomials of degree 3, and **quartic** terms denote polynomials of degree 4.

We can think of polynomials as functions of x. The variable x does not necessarily need to come from the same set as the polynomial's coefficients; for example, we can plug in $x = i$ into the polynomial $f(x) = x^2 + 2$ to get $f(i) = 1$.

However, polynomials are interesting in their own right, not just as functions. Polynomials have their own arithmetic, which we'll discuss now. For the sake of clarity, we will define $P(X) = p_0 + p_1x + \dots p_nx^n$ and $Q(x) = q_0 + q_1x + \dots q_mx^m$.

> *Remark.* The reason for the capital X is that we're referring to polynomials as objects rather than functions of x when we define arithmetic on them, though the distinction isn't that important for our purposes.

Definition 4.3. Polynomial Addition Without loss of generality, assume $n \geq m$. Then,

$$P(X) + Q(X) = (p_0 + q_0) + (p_1 + q_1)x + \dots (p_m + q_m)x^m + \dots p_nx^n$$

with subtraction being defined similarly. Next, we define multiplication:

Definition 4.4. Polynomial Multiplication Without loss of generality, assume $n \geq m$. Then,

$$P(X)Q(X) = p_0q_0 + (p_1q_0 + p_0q_1)x + (p_2q_0 + p_1q_1 + p_0q_2)x^2 + \dots p_nq_mx^{m+n}$$

In regular integer arithmetic, division has quotients and remainders. For example, if we divide 7 by 3, we get a quotient of 2 and remainder 1, since $7 = 3 * 2 + 1$. Putting in this a polynomial perspective, suppose by we divide $F(X)$ by $P(X)$.

Definition 4.5. Polynomial division If $F(X)$ is a polynomial being divided by $P(X)$, we express this as

$$F(X) = P(X)Q(X) + R(X)$$

where $\deg(R(X)) \leq \deg(P(X)) - 1$.

In this case, $Q(X)$ represents the quotient while $R(X)$ represents the remainder. The requirement that $\deg(R(X)) \leq \deg(P(X)) - 1$ ensures that our remainder is "smaller" than our divisor. For example, if you divide a cubic by a quadratic, the remainder must either be linear or a constant.

§4.1.1 Polynomial Long Division

Polynomial long division is similar to regular long division, except instead of tens places, we have powers of x. It is an important tool for factoring polynomials; if you know that $x - r$ is a factor of a polynomial $f(x)$, then you can use polynomial division to find $q(x) = f(x)/(x - r)$ and factor $f(x)$ into $(x - r)q(x)$.

If you're not familiar with polynomial long division, we recommend that you learn this using other online resources, as it should be fairly easy. However, we'll show a few examples here as a refresher.

Example. Find the quotient and remainder when $x^4 + 4x^2 + 5x + 3$ is divided by $x^2 + 1$.

Using polynomial long division, we get

$$\begin{array}{r} x^2 \quad +3 \\ \hline x^2+1 \big) \; x^4+4x^2+5x+3 \\ \underline{-x^4 \quad -x^2} \\ 3x^2+5x+3 \\ \underline{-3x^2 \quad -3} \\ 5x \end{array}$$

So our quotient is $x^2 + 3$ and our remainder is $5x$.

Example. Find the remainder when $x^4 + 5x^3 + x^2 + 8x + 11$ is divided by $x^2 + 2x + 1$.

Solution. Notice that $x^2 + 2x + 1 = (x + 1)^2$. Then, we can first divide by $x + 1$, then divide the result by $x + 1$.

$$\begin{array}{r} x^3+4x^2 \quad -3x+11 \\ \hline x+1 \big) \; x^4+5x^3 \quad +x^2 \quad +8x+11 \\ \underline{-x^4 \quad -x^3} \\ 4x^3 \quad +x^2 \\ \underline{-4x^3-4x^2} \\ -3x^2 \quad +8x \\ \underline{3x^2 \quad +3x} \\ 11x+11 \\ \underline{-11x-11} \\ 0 \end{array}$$

Note that we first multiplied by x^3. Then, we can divide again by $x + 1$ to get our answer:

$$\begin{array}{r} x^2+4x \quad -7 \\ \hline x+1 \big) \; x^3+5x^2-3x+11 \\ \underline{-x^3 \quad -x^2} \\ 4x^2-3x \\ \underline{-4x^2-4x} \\ -7x+11 \\ \underline{7x \quad +7} \\ 18 \end{array}$$

Hence, our remainder is 18. ■

The **remainder theorem** is an important theorem pertaining to polynomial division.

Theorem 4.6 (Remainder Theorem). *Assume we have a polynomial $F(X)$ being divided by*

a linear polynomial $P(X) = ax + b$. If $R(X)$ is the remainder polynomial as a result of this division, then we have $R(X) = F\left(-\frac{b}{a}\right)$.

Proof. We first start with our expression for polynomial division, and let $P(X) = ax + b$. Note that this makes $R(X)$ a constant as it must have degree less than 1. Then, we have that

$$F(X) = (ax + b)Q(X) + R(X).$$

Clearly, since $a(-\frac{b}{a}) + b = -b + b = 0$, if we plug in $X = -\frac{b}{a}$ then we have that

$$F\left(-\frac{b}{a}\right) = 0 + R\left(-\frac{b}{a}\right)$$
$$F\left(-\frac{b}{a}\right) = R\left(-\frac{b}{a}\right).$$

But since $R(X)$ is constant, $R(X) + R(-\frac{b}{a})$, so

$$F\left(-\frac{b}{a}\right) = R(X)$$

and we are done. ■

Though the remainder theorem in itself is mostly a trick to save time, we can apply the fundamental idea of the remainder theorem— that plugging in roots simplifies division expressions greatly— to solve problems.

Example 4.7 (BMC). Find the remainder when $x^{81} + x^{49} + x^{25} + x^9 + x$ is divided by $x^3 - x$.

Solution. We first make our polynomial division expression:

$$x^{81} + x^{49} + x^{25} + x^9 + x = (x^3 - x)Q(x) + R(x)$$

Since we are dividing by $x^3 - x$, this means that $\deg(R(X))$ is at most 2. Hence, we can let $R(X) = ax^2 + bx + c$ for some constants a, b, c.

Now, although we haven't covered roots yet, the next part is fairly intuitive. We need three values of $R(X)$ as we have 3 variables to solve for. However, if we were to say choose some arbitrary $x = 2$, then we have the huge equation

$$2^{81} + 2^{49} + 2^{25} + 2^9 + 2 = (2^3 - 2)Q(2) + R(2).$$

There are two major problems: the numbers are huge and we actually have no idea what $Q(x)$ is, let alone $Q(2)$.

However, we know $Q(x)$ is being multiplied by $x^3 - x$. Thus, we can at least eliminate one major problem by setting $x^3 - x = 0$ so we don't need to deal with $Q(x)$. Hence, we solve for the different values of x :

$$x^3 - x = 0$$
$$x(x^2 - 1) = 0$$
$$x(x - 1)(x + 1) = 0$$

The values of x that satisfy this equation are $0, 1, -1$ which is also very convenient because this eliminates our other major problem: huge numbers. Plugging in these three values into the expression, we get the following system of equations:

$$\begin{aligned} R(1) &= a + b + c = 5 \\ R(0) &= c = 0 \\ R(-1) &= a - b + c = -5 \end{aligned}$$

Solving this systems of equations gives $a = 0, b = 5, c = 0$. Hence, our remainder is 5x. ■

§4.2 Roots

Perhaps one of the most important concepts of polynomials are their roots. Why should we care about when a polynomial is equal to 0? Well, the most obvious point comes directly from the zero product property.

Theorem 4.8 (Factor Theorem). *A number r is a root of the polynomial $P(x)$ if and only if $x - r$ is a factor of $P(x)$.*

Proof. First, we'll prove the forwards direction: if r is a root of $P(x)$, then $P(r) = 0$. Assume the degree of P is n. Write $P(x)$ as

$$P(x) = a(x - r_1)(x - r_2) \cdots (x - r_n)$$

so that $r_1, r_2, \cdots, r_n$ are the roots of P. Then, as $P(r) = 0$, we know that $a(r-r_1) \cdots (r-r_n) = 0$, so at least one of $r - r_1, \cdots, r - r_n$ must be equal to 0 by the zero product property; therefore $r = r_i$ for some i between 1 and n. It follows indeed that $x - r$ is a factor of $P(x)$, as desired, as all the $x - r_i$'s are factors of $P(x)$.

Now, if $x - r$ is a factor of $P(x)$, then $P(x) = (x - r)Q(x)$ for some other polynomial $Q(x)$. It follows that $P(r) = (r - r)Q(r) = 0$, so therefore f is a root of $P(x)$, as desired. ■

There is another fact that makes roots important.

Theorem 4.9 (Fundamental Theorem of Algebra). *A polynomial $P(x)$ of degree n has n roots in total, real and complex.*

This allows us to express any polynomial P as

$$P(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n)$$

where $r_1, \cdots, r_n$ are the roots of P, and a_n is its leading coefficient.

Exercise. Prove the above statement using the fundamental theorem of algebra and the factor theorem. (If you want to do this formally, you might have to use induction!)

Note that roots can appear more than once in the factorization of a polynomial. For example, $x^2-2x+1 = (x-1)^2$, which has two factors of $x-1$. To deal with this, we define **multiplicity**. A root r has multiplicity k if $(x-r)$ appears exactly k times in the factorization of the polynomial. When we say a polynomial has roots $r_1, r_2, \ldots r_n$, they are **not** assumed to be distinct; if a root has multiplicity k, then it appears k times in $r_1, r_2, \ldots r_n$.

§4.2.1 Vieta's

We know how to factor polynomials with rational roots, like quadratics. Whenever we can directly find roots, we should do so. Unfortunately, we will often be given problems where directly finding roots is impossible. Thankfully, it turns out that we can still figure out a lot about the roots of a polynomial without knowing what they are.

Specifically, the fact that we can break down a polynomial into its linear factors $(x-r_i)$ gives rise to a very important series of formulas known as Vieta's formulas. Before we get into Vieta's formulas, though, we first have to define symmetric sums.

Definition 4.10. Define the ***k*th elementary symmetric sum** of n variables $a_1, a_2, \cdots, a_n$ as the sum of all combinations of products of k of these variables at a time. We'll denote this as S_k. (The original number of variables will be clear from context.)

Of course, it's hard to understand this without some examples. The first elementary symmetric sum of any n variables $a_1, \cdots, a_n$, denoted S_1, is just

$$S_1 = a_1 + a_2 + \cdots + a_n.$$

The second, S_2, is

$$S_2 = a_1a_2 + a_1a_3 + \cdots + a_{n-1}a_n,$$

where S_2 is the sum of all products of all pairs of elements.

Here a few specific cases: if there are five variables a, b, c, d, and e, then

$$S_4 = abcd + abce + abde + acde + bcde.$$

If there are four variables a, b, c, and d, then

$$S_2 = ab + ac + ad + bc + bd + cd$$

and

$$S_4 = abcd.$$

Theorem 4.11 (Vieta's Formulas). *Given a polynomial $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with roots $r_1, r_2, \cdots, r_n$, **Vieta's Formulas** state that*

$$S_k = (-1)^k \cdot \frac{a_{n-k}}{a_n},$$

where S_k denotes the kth elementary symmetric sum of the roots $r_1, \cdots, r_n$.

Proof. We know that we can express $P(x)$ as

$$P(x) = a(x - r_1)(x - r_2)\cdots(x - r_n)$$

for some constant a. In this case, it is clear that $a = a_n$.

Expanding this yields

$$\begin{aligned} P(x) = a_nx^n &+ a_n(-r_1 - r_2 - \cdots - r_n)x^{n-1} \\ &+ a_n(r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n)x^{n-2} \\ &+ \ \ldots \ + (-r_1)(-r_2)\cdots(-r_n). \end{aligned}$$

Look at these coefficients. Miraculously, they're the elementary symmetric sums of the n roots. Additionally, depending on which coefficient we're dealing with, we have a power of -1 to deal with — and as such, by comparing coefficients,

$$a_n(S_k)(-1)^k = a_{n-k}.$$

This rearranges to the desired equation. ■

Now let's try some examples.

Example 4.12. For the polynomial $x^4 + 5x^2 + 8x + 9$, find the sum and product of all of its roots.

Solution. We first solve for the sum of all of the roots. We know that $a_4 = 1$, $a_3 = 0$, $a_2 = 5$, $a_1 = 8$, and $a_0 = 9$. From Vieta's, we have that

$$r_1 + r_2 + r_3 + r_4 = -\frac{a_3}{a_4} = -\frac{0}{1} = 0,$$

so the sum of all of the roots is 0. Similarly, the product of all of the roots is

$$r_1 r_2 r_3 r_4 = (-1)^4 \cdot \frac{9}{1} = 9.$$

Thus, the product of all of our roots is 9. ■

Example 4.13. If p, q, r, and s are the roots of $P(x) = 2x^4 - 6x^3 - 30x^2 + 12x + 10$, then find

1. $p + q + r + s$,
2. $pq + pr + ps + qr + qs + rs$,
3. $pqr + pqs + prs + qrs$, and
4. $pqrs$.

Solution. We know that $p+q+r+s = S_1$, the first elementary symmetric sum, so our answer is

$$S_1 = (-1) \cdot \frac{-6}{2} = 3.$$

Next, $pq + pr + ps + qr + qs + rs = S_2$, so our answer is

$$S_2 = (-1)^2 \cdot \frac{-30}{2} = -15.$$

Now, $pqr + pqs + prs + qrs = S_3$, so our answer is

$$S_3 = (-1)^3 \cdot \frac{12}{2} = -6.$$

Finally, $pqrs = S_4$, so our answer is

$$S_4 = (-1)^4 \cdot \frac{10}{2} = 5.$$

■

It is important to remember that Vieta's Formulas only apply to polynomials; however, it is sometimes possible to manipulate equations to turn them into polynomials, as we will see in the following example:

Example 4.14. (2003 AMC 10A) What is the sum of the reciprocals of the roots of the equation $\frac{2003}{2004}x + 1 + \frac{1}{x} = 0$?

Solution. We want to find a symmetric expression containing all the roots, so Vieta's Formula should come to mind. However, we cannot apply Vieta's immediately, as $\frac{2003}{2004}x + 1 + \frac{1}{x}$ is not a polynomial. We can multiply both sides of the equation by x to get rid of the $\frac{1}{x}$, and instead find the roots of

$$\frac{2003}{2004}x^2 + x + 1 = 0.$$

We must ensure $x = 0$ is not a root (otherwise we would be dividing by zero in the original equation).

It is easy to see that it is not, so we can apply Vieta's without worrying about extraneous roots.

Let the roots of this equation be x_1 and x_2. We are asked to find the sum of the reciprocals of the roots, or

$$\frac{1}{x_1} + \frac{1}{x_2} = \frac{x_1 + x_2}{x_1 x_2}.$$

$x_1 + x_2 = \frac{-1}{\frac{2004}{2003}}$ and $x_1 \cdot x_2 = \frac{1}{\frac{2004}{2003}}$, so our answer is

$$\frac{\left(\frac{-1}{\frac{2004}{2003}}\right)}{\left(\frac{1}{\frac{2004}{2003}}\right)} = \frac{-1}{1} = -1.$$

■

Remark. If we have a polynomial $f(x)$ with degree n (so $f(x)$ has n roots $r_1, \ldots, r_n$) then a common trick for finding the sum of the reciprocals of the roots is using the fact that

$$\frac{1}{r_1} + \frac{1}{r_2} + \cdots + \frac{1}{r_n} = -\frac{S_{n-1}}{S_n}.$$

Example 4.15. If r, s, t are the three roots of polynomial $f(x) = x^3 + 5x^2 - 8x + 9$, find $(r + s + 1)(s + t + 1)(t + r + 1)$.

Solution. It seems rather tempting to just expand out the terms. After all, we already know that

$$\begin{aligned} r + s + t &= -5 \\ rs + st + tr &= 8 \\ rst &= -9 \end{aligned}$$

so we can just group together the terms and plug and chug. And while this certainly is a viable solution, there exists a much cleaner and efficient way. We know that we can express any cubic polynomial as

$$f(x) = a_n(x - r_1)(x - r_2)(x - r_3).$$

Since the leading coefficient of $f(x)$ is 1, we have that $a_n = 1$ and we know that our roots are r, s, t so we can express $f(x)$ as

$$f(x) = (x - r)(x - s)(x - t).$$

We know we can substitute any x. Note the symmetry of $(r + s + 1)(s + t + 1)(t + r + 1)$. If we let $x = r + s + t + 1$, we then find that

$$f(r + s + t + 1) = (s + t + 1)(t + r + 1)(r + s + 1)$$

which is exactly what we need to find! We even know $r + s + t$ from Vieta's, which is -5, so we just need to calculate $f(-5 + 1) = f(-4)$. This is the easiest step: we just evaluate our polynomial with $x = -4$. Doing so gives us

$$-64 + 80 + 32 + 9 = 57$$

as our answer. ■

Whenever applying Vieta's, don't forget to include the alternating signs, and make sure you remember to divide by the leading coefficient as not every polynomial given will be monic (i.e. have leading coefficient 1).

We'll move on to a problem that's much harder than the previous examples, but should still be solveable with our tools.

Example 4.16. (2017 AMC 10A) For certain real numbers a, b, c the polynomial

$$g(x) = x^3 + ax^2 + x + 10$$

has three distinct roots, and each root of $g(x)$ is also a root of the polynomial

$$f(x) = x^4 + x^3 + bx^2 + 100x + c.$$

What is $f(1)$?

Solution. Note that since $f(x)$ and $g(x)$ are both monic and they share 3 roots, we can set up the following equation

$$f(x) = (x - r)g(x)$$

for some real r. Now, we can substitute in $g(x)$ and then compare coefficients with $f(x)$:

$$f(x) = (x - r)(x^3 + ax^2 + x + 10)$$
$$f(x) = x^4 + (a - r)x^3 + (1 - ar)x^2 + (10 - r)x - 10r$$

This gives us

$$x^4 + x^3 + bx^2 + 100x + c = x^4 + (a - r)x^3 + (1 - ar)x^2 + (10 - r)x - 10r.$$

By matching coefficients, we can set up a system of four equations:

$$a - r = 1$$
$$1 - ar = b$$
$$10 - r = 100$$
$$-10r = c$$

Before we start solving for any values, let's first examine the problem statement so we know exactly what we need to do. The problem says to find $f(1)$, and plugging in 1 gives us $1+1+b+100+c$, so we need to find b and c. Let's get right into it.

From the third equation, we find that $r = -90$. Thus, we can directly plug this into the fourth equation to get $c = 900$.

Now, it remains to find the value of b. From the first equation, we obtain that $a-(-90) = 1$, so $a = -89$. Then, plugging this into the second equation gives $1-(-90)(-89) = b$. So, $b = -8009$.

Finally, we can plug in all the values we got. Our final answer is $1 + 1 - 8009 + 100 + 900$ which conveniently simplifies down to -7007.

■

Now, we'll introduce another application of Vieta's formulas, **Newton Sums**. Newton Sums are a method of expressing $p_n = a^n + b^n + c^n$ as a combination of symmetric sums and lower power sums like p_{n-1} and p_{n-2}.

Theorem 4.17 (Newton Sums). *Suppose that we are given a polynomial $P(x) = \sum_{i=0}^{n} a_n x^n$, where $a_n \neq 0$. Denote the nth symmetric sum by S_n. Given that $x_1, x_2, ..., x_n$ are the roots of $P(x)$, let P_n denote $\sum_{i=1}^{n} x_i^n$. Then, for all $1 \leq m \leq n$,*

$$(-1)^m m S_m + \sum_{k=1}^{m} (-1)^{k+m} P_k S_{m-k} = 0.$$

The first few indentites are as follows:

1. $P_1 = S_1$
2. $P_2 = S_1 P_1 - 2S_2$
3. $P_3 = S_1 P_2 - S_2 P_1 + 3S_3$
4. $P_4 = S_1 P_3 - S_2 P_2 + S_3 P_1 - 4S_4$

You can ignore the scary sum and just focus on the pattern in the identities.

The proof is quite long and tedious, but if you want to prove it on your own, try plugging in all the roots of $P(x)$, set these expressions equal to 0, then use Vieta's to express the coefficients in terms of the roots.

Note that if we only have 3 variables, then S_4 is just 0, and we can further ignore any expressions with S_5 and so forth.

The following is a very nice problem that utilizes a small amount of trig. For now, if you have not learned trig, do not look at the solution and add $\sin^2 x + \cos^2 x = 1$ to your workspace to further attempt the problem.

Example 4.18. (2019 AIME) Let x be a real number such that $\sin^{10} x + \cos^{10} x = \frac{11}{36}$. Then, $\sin^{12} x + \cos^{12} x = \frac{m}{n}$. where $\frac{m}{n}$ is in lowest terms. Find $m + n$.

Solution. To simplify your work, it is very easy to simply let $\sin^2 x = a$ and $\cos^2 x = b$. Thus, we also have that $a + b = 1$ by the Pythagorean identity and we are given $a^5 + b^5 = \frac{11}{36}$. We are looking for $a^6 + b^6$.

We can now apply Newton sums– you may wonder why, because there's no polynomial in this problem, and Newton sums are usually given in that context.

However, if you glance at the identities again, you will see we're only concerned with symmetric sums and power sums. We have our power sums directly from the problem, and since we only have two variables, our only symmetric sums are $s_1 = a + b = 1$ and $s_2 = ab$. Thus, we can use the information we get using Newton sums to solve for s_2 and then get the value of $p_6 = a^6 + b^6$, which is what we're looking for.

We know that $s_1 = p_1 = 1$. Hence, we have that

$$\begin{aligned} p_6 &= s_1 p_5 - s_2 p_4 \\ p_5 &= s_1 p_4 - s_2 p_3 \\ p_4 &= s_1 p_3 - s_2 p_2 \\ p_3 &= s_1 p_2 - s_2 p_1 \\ p_2 &= s_1 p_1 - 2s_2 \end{aligned}$$

Note that we're just taking the identities for the first six power sums and ignoring the terms with symmetric sums higher than the second symmetric sum.

So, we want to further simplify p_5's expression as we already know its value. To also simplify the visuals, we also let $s_2 = c$. Note that $p_2 = 1 - 2c$.

$$\begin{aligned} \frac{11}{36} &= p_4 - c(s_1 p_2 - c p_1) \\ \frac{11}{36} &= (p_3 - c p_2) - c(p_2 - c) \\ \frac{11}{36} &= (p_2 - c - c p_2) - c p_2 + c^2 \\ \frac{11}{36} &= 5c^2 - 5c + 1 \end{aligned}$$

So, we now have a handy in one variable. Now, we solve for c. If you are unfamiliar with quadratics, you can skim over the next section, but the solution doesn't require anything fancy.

$$\begin{aligned} 5c^2 - 5c + \frac{25}{36} &= 0 \\ 36c^2 - 36c + 5 &= 0 \\ (6c - 5)(6c - 1) &= 0 \end{aligned}$$

Thus, we either get $c = \frac{5}{6}$ or $c = \frac{1}{6}$. If you don't have a trig background, take our word that $c = \frac{5}{6}$ is impossible. The reason why is because

$$c = \sin^2 x \cdot \cos^2 x = \frac{\sin^2(2x)}{4}$$

However, $\sin^2(2x) < 1$, so $c < \frac{1}{4}$ which is why $c = \frac{1}{6}$. Now armed with this knowledge, we can simply plug and chug. After solving for p_4, which is $\frac{7}{18}$, we have that $p_6 = \frac{13}{54}$.

■

§4.3 Quadratics

Let's now examine one of the most commonly seen polynomials: quadratics. While the name might be a bit misleading as "quad" generally means 4, a quadratic equation is any polynomial with degree 2. Formally, it is any $f(x) = ax^2 + bx + c$ where a, b, and c are real numbers and $a \neq 0$. Quadratics are very nice and a great introduction to solving roots because there exists a handy formula called the...

Theorem 4.19 (Quadratic Formula). *The solutions of the equation* $ax^2 + bx + c = 0$ *are*

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

.

Proof of Theorem 4.19. We utilize a technique called "completing the square." That is, we wish to create a squared term $z(x-y)^2$ for constants z, y as this allows us to take the square root of an equation and thereby reduce the degree of our x terms by 1.

$$\begin{aligned} & ax^2 + bx + c = 0 \\ \iff & a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = 0 \\ \iff & a\left(\frac{b^2}{4a^2} - \frac{c}{a}\right) = a\left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}\right) \\ \iff & \frac{b^2 - 4ac}{4a^2} = x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \left(x + \frac{b}{2a}\right) \\ \iff & \boxed{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}} \end{aligned}$$

■

The quadratic formula allows us to directly compute roots, which makes factoring larger polynomials even more potent as we only really need to factor into quadratics to compute all roots.

We call the part containing the radical, $\sqrt{b^2 - 4ac}$, the **discriminant**.

Proposition 4.20 (Discriminant). *Let* $D = \sqrt{b^2 - 4ac}$. *The quadratic* $ax^2 + bx + c$ *has two real solutions when* $D > 0$, *one real solution when* $D = 0$, *and no real solutions when* $D < 0$.

Exercise. Prove Proposition 4.20.

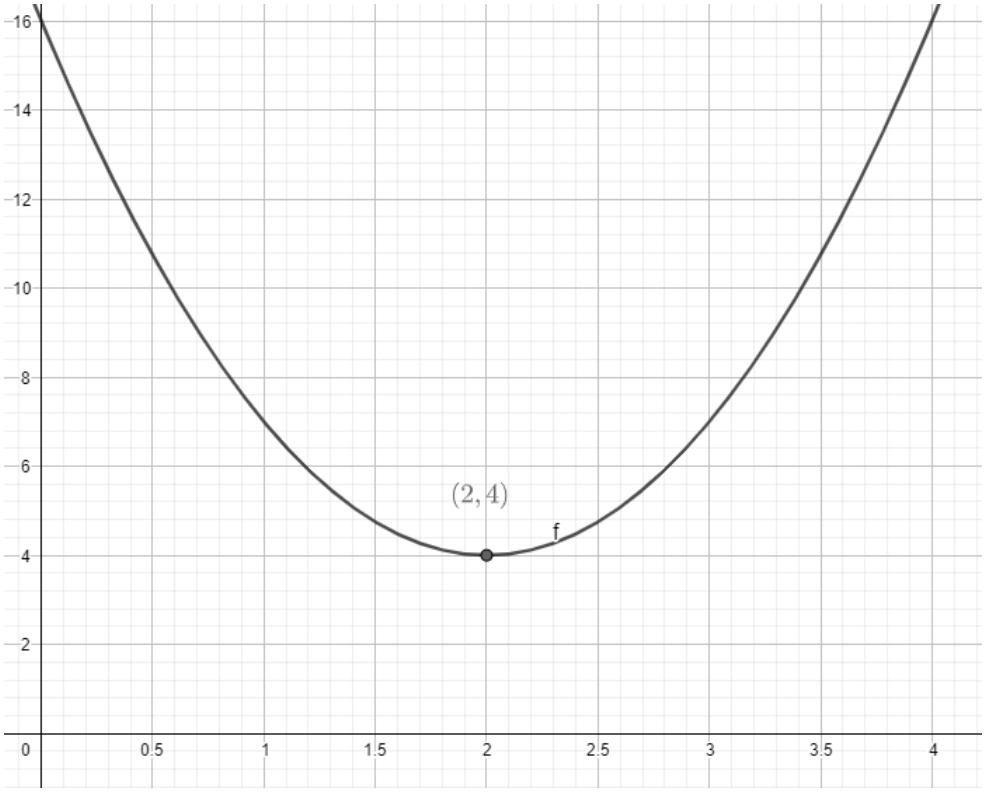
We've established some nice algebraic facts about quadratics. However, it is also useful to think about quadratics from a graphical perspective. We start with **vertex form**:

$$y = a(x - h)^2 + k$$

This is called vertex form because this directly gives us the vertex of the parabola: (h, k). To think about why this is the vertex, suppose $x = h$. If $a > 0$, then if $x < h$ or $x > h$ will yield a positive value of $(x - h)^2$, hence any other value of x will make the y greater than when $x = h$. Similar reasoning applies when $a < 0$.

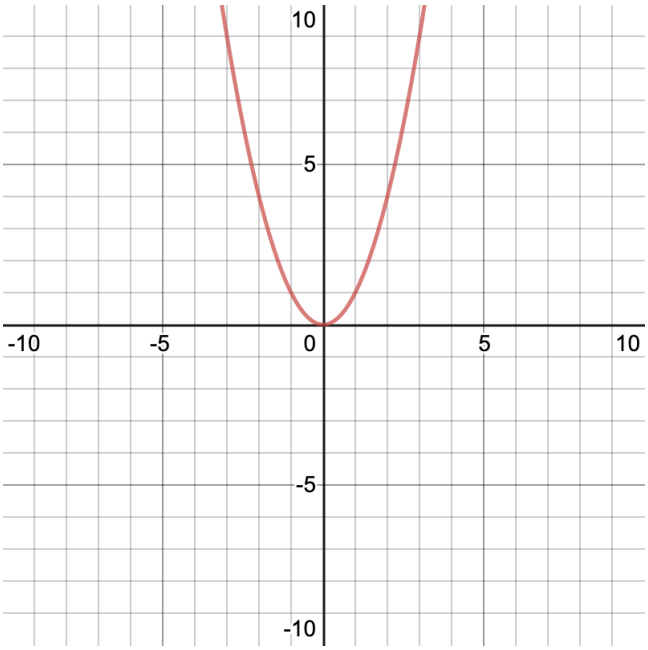
Vertex form can be obtained from the **standard form** of a quadratic, $y = ax^2 + bx + c$, by completing the square (the same method we used in the proof of the quadratic formula).

As an example, here is the graph of $y = 3(x - 2)^2 + 4$:



Now we'll talk about the graphical implications of the discriminant.

We know that if $D > 0$, a quadratic has two real solutions, so it intersects the x-axis twice. If $D = 0$, then it is tangent to the x-axis (i.e. it touches the x-axis but does not pass through it). For example, here is the graph of $y = x^2$:



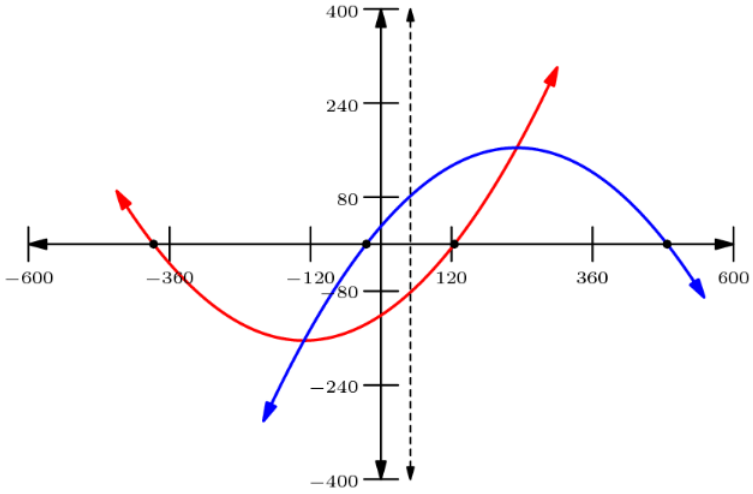
Note how it touches the x-axis, but bounces off. This behavior occurs in any quadratic with discriminant 0.

Finally, if the discriminant is less than 0, the quadratic never touches or passes through the x-axis.

Now let's apply our knowledge of quadratics to some problems.

Example 4.21. (2009 AMC 12A) Functions f and g are quadratic, $g(x) = -f(100 - x)$, and the graph of g contains the vertex of the graph of f. The four x-intercepts on the two graphs have x-coordinates x_1, x_2, x_3, and x_4, in increasing order, and $x_3 - x_2 = 150$. The value of $x_4 - x_1$ is $m + n\sqrt{p}$, where m, n, and p are positive integers, and p is not divisible by the square of any prime. What is $m + n + p$?

Solution. Something that can immediately observed is a kind of symmetry about $x = 50$. Substituting in $50 - x$ for x gives us that $g(50 - x) = -f(50 + x)$.



AoPS

Thus, if a is a point a distance of x to the left of 50, and b is a point a distance of x to the right of 50, we know that $g(a) = -f(b)$.

Thus, we can simplify our calculations by simply shifting our graph to the left by 50. Instead of $g(x)$ and $f(x)$ being symmetric about $x = 50$, they are now centered about the y-axis! The question asks for the distance between two roots. Since we translated every point equally, distance should be preserved, so we don't need to worry about doing this.

Then we know that $x_3 = -x_2$ since both roots must be equidistant from the y-axis.

Thus, $x_3 = (75, 0)$ and $x_2 = (-75, 0)$. We know that we can express a quadratic as

$$f(x) = a(x - r_1)(x - r_2)$$

for roots r_1 and r_2 as well as constant a. For the sake of simplicity, suppose $x_4 = -b$. Applying this expression to both $f(x)$ and $g(x)$ gives:

$$f(x) = a(x - 75)(x - b)$$
$$g(x) = -a(x + 75)(x + b)$$

Note that it doesn't matter if $f(x)$ gets the negative or positive root - symmetry will give the same results either way. From here, we want to use the info that $g(x)$ contains the vertex of $f(x)$. So, we get the vertex form of $f(x)$.

$$f(x) = ax^2 - a(75 + b)x + 75ab$$

Thus, $\frac{75+b}{2}$ is the x value of our vertex. Hence, we have the following relationship:

$$p\left(\frac{75+b}{2}\right) = q\left(\frac{75+b}{2}\right)$$

Plugging this into $p(x)$ and $q(x)$ respectively gives:

$$p\left(\frac{75+b}{2}\right) = a\left(\frac{-75+b}{2}\right)\left(\frac{75-b}{2}\right)$$
$$q\left(\frac{75+b}{2}\right) = -a\left(\frac{225+b}{2}\right)\left(\frac{75+3b}{2}\right)$$

Setting these two equal to each other and then simplifying gives:

$$\left(\frac{-75+b}{2}\right)\left(\frac{75-b}{2}\right) = -\left(\frac{225+b}{2}\right)\left(\frac{75+3b}{2}\right)$$
$$(-75+b)(75-b) = -(225+b)(75+3b)$$
$$b^2 - 150b + 75^2 = 3\cdot 75^2 + 3b^2 + 750b$$
$$2b^2 + 900b + 2\cdot 75^2 = 0$$

Thus, we get that $b^2 + 450b + 75^2 = 0$. Applying the quadratic formula gives:

$$b = \frac{-450 \pm \sqrt{450^2 - 150^2}}{2}$$

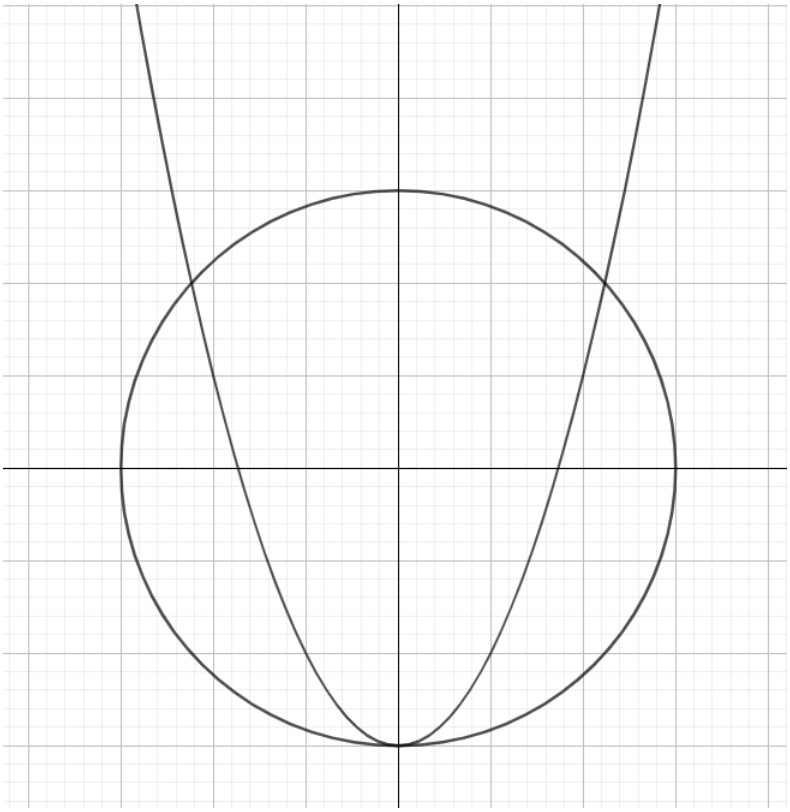
Further simplifying this expression gives:

$$b = \frac{-450 \pm 150\sqrt{3^2 - 1^2}}{2}$$
$$b = -225 \pm 150\sqrt{2}$$

The magnitude of b must be larger than 75 since b and $-b$ will be our roots x_1 and x_4. Then we have that $b = -225 - 150\sqrt{2}$. Thus, we are looking for $x_4 - x_1 = -b - (b) = -2b = 450 + 300\sqrt{2}$. Then the answer is $450 + 300 + 2 = 752$. ■

Example 4.22. (2018 AMC 10A) Find the interval for the set of values of a such that the curves $x^2 + y^2 = a^2$ and $y = x^2 - a$ in the real xy-plane intersect at exactly 3 points.

Solution. We begin by drawing the diagram. Note that this problem will require the reader to know the general equation for a circle. Conveniently, they gave our quadratic already in vertex form, so we can derive that the vertex is $(0, -a)$. Moreover, simply by plugging in $(0, -a)$ into $x^2 + y^2$ gives a^2, so we know that there already is one intersection between the parabola and circle.



So, we just need to make sure that our parabola only intersects the circle at 2 more points, requiring the curve to be "inside" of the circle. In your own time, try playing around with values of a to see how the graph adjusts. The easiest way to do so is to first see what happens when we assume that the circle and parabola intersect.

We first set the two equations to each other, but in order to simplify calculations we instead substitute $x^2 = y + a$ into the first equation to get

$$y^2 + y + a = a^2.$$

We can then manipulate the equation to get

$$y^2 + y + 1 = a^2 - a + 1.$$

From here, we complete the square on both sides:

$$\left(y + \frac{1}{2}\right)^2 = \left(a - \frac{1}{2}\right)^2$$

From here, we can break this down into two cases:

$$y + \frac{1}{2} = a - \frac{1}{2}$$
$$y + \frac{1}{2} = -(a - \frac{1}{2})$$

We'll first work with the second case. In this case, we have that $y = -a$. However, this doesn't give us any information as we already know that $(0, -a)$ is an intersection.

Now, we return to the first case. We obtain that $y = a - 1$, and then we can substitute this into the quadratic:

$$(a - 1) = x^2 - a$$
$$2a - 1 = x^2$$

x will have 2 solutions as long as $2a - 1 > 0$ which is what we want as we need 3 total intersections. Hence, this gives the desired interval $a > \frac{1}{2}$.

Note that you don't need to draw the diagram and could directly go into calculating the intersections between the two curves; outside of stimulating intuition or ideas, it didn't have much purpose. ■

§4.4 Homework Problems

Problem 4.1 (2000 AMC12)**.** [4]Let f be a function for which $f(x/3) = x^2 + x + 1$. The the sum of all values of z for which $f(3z) = 7$ is a fraction $-\frac{m}{n}$ for relatively prime positive integers m and n. Find $m + n$.

Problem 4.2 (2010 AMC 10A)**.** [5] The polynomial $x^3 - ax^2 + bx - 2010$ has three positive integer roots. What is the smallest possible value of a?

Problem 4.3 (2007 AMC 10A)**.** [5] Suppose that the number a satisfies the equation $4 = a + a^{-1}$. What is the value of $a^4 + a^{-4}$?

Problem 4.4 (2014 AIME II)**.** [6] Real numbers r and s are roots of $p(x) = x^3 + ax + b$, and $r + 4$ and $s - 3$ are roots of $q(x) = x^3 + ax + b + 240$. Find the sum of all possible values of $|b|$.

Problem 4.5 (2019 AMC 12A)**.** [6] Let s_k denote the sum of the kth powers of the roots of the polynomial $x^3 - 5x^2 + 8x - 13$. In particular, $s_0 = 3$, $s_1 = 5$, and $s_2 = 9$. Let a, b, and c be real numbers such that $s_{k+1} = a\,s_k + b\,s_{k-1} + c\,s_{k-2}$ for $k = 2, 3, ...$ What is $a + b + c$?

Problem 4.6 (2001 AMC12)**.** [6] The polynomial $p(x) = x^3 + ax^2 + bx + c$ has the property that the average of its zeros, the product of its zeros, and the sum of its coefficients are all equal. The y-intercept of the graph of $y = p(x)$ is 2. What is $|b|$?

Problem 4.7 (1991 AIME Problem)**.** [8] For how many real numbers a does the quadratic equation $x^2 + ax + 6a = 0$ have only integer roots for x?

Problem 4.8 (2003 AIME II)**.** [10] Consider the polynomials $P(x) = x^6 - x^5 - x^3 - x^2 - x$ and $Q(x) = x^4 - x^3 - x^2 - 1$. Given that z_1, z_2, z_3, and z_4 are the roots of $Q(x) = 0$, find $P(z_1) + P(z_2) + P(z_3) + P(z_4)$.

Show your work for this problem, and include any progress even if you didn't manage to solve it!

5 Trigonometry and Complex Numbers

In this handout, we'll go over basic trig and trig identities. We'll also cover complex numbers and Euler's formula, where our knowledge of trig will come in handy.

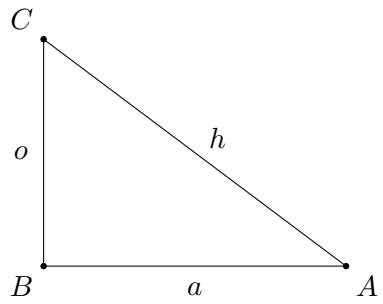
Radians

Before we get into examples, we'll first define **radians**, the SI(standard) unit of angle measurement. Instead of having 360 degrees, a circle has 2π radians. This is a more useful unit than degrees because the length of the arc of a unit circle is equal to the angle it subtends when measured in radians.

It's common convention to use radians when dealing with trigonometric functions, mainly because the more natural definition allows us to formulate results a lot more easily and elegantly in fields that use trig like complex analysis

§5.1 Trigonometric Functions

We'll define trigonometric functions using a right triangle. Suppose that $\triangle ABC$ has $\angle B = \frac{\pi}{2}$; then we label side BC as the side **opposite** of angle $\angle A$, and we label side AB as the side **adjacent** to angle $\angle A$.



The basic trigonometric functions are then defined as follows:

Function Name	Symbol	Value
sine	$\sin(\angle A)$	$\frac{BC}{AC}$
cosine	$\cos(\angle A)$	$\frac{AB}{AC}$
tangent	$\tan(\angle A)$	$\frac{AB}{AC}$
cosecant	$\csc(\angle A)$	$\frac{AB}{AC}$
secant	$\sec(\angle A)$	$\frac{AB}{AC}$
cotangent	$\cot(\angle A)$	$\frac{AB}{AC}$

A nice mnemonic to remember these formulas is SOH CAH TOA – **S**ine is **O**pposite over **H**ypotenuse, **C**osine is **A**djacent over **H**ypotenuse, and **T**angent is **O**pposite over **A**djacent. We can also observe right off the bat that

$$\tan(\angle A) = \frac{\sin(\angle A)}{\cos(\angle A)}$$

$$\sin(\angle A) = \cos(\angle B) = \sin(90^\circ - \angle B)$$

Similar relations hold for the other trig functions. We also see that

$$\csc(\angle A) = \frac{1}{\sin(\angle A)}$$
$$\sec(\angle A) = \frac{1}{\cos(\angle A)}$$
$$\cot(\angle A) = \frac{1}{\tan(\angle A)}$$

Thus, we're mainly going to be focusing on sine and cosine identities, since the other trig functions can all be expressed in terms of these two.

Exercise 5.1. Show that $\sin(\frac{\pi}{3}) = \frac{\sqrt{3}}{2}$ and that $\cos(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}$.

Hint: View some common triangles with relevant angles.

Though $f^2(x)$ usually means $f(f(x))$ in the context of functions, this notation is instead used for exponentiation when we're dealing with trig functions; thus, $\sin^2 x = \sin x \cdot \sin x$. However, the convention for inverse is still the same (so that $\sin^{-1}(\sin(x)) = x$ and $\sin(\sin^{-1}(x)) = x$ for x in the correct domains).

This can get confusing, so mathematicians often prefix an arc in front of trig functions to denote inverses instead, such as $\arcsin(\sin(x)) = x$. We will be using this notation for the rest of the handout. We also will omit the parentheses when it's obvious what the input is. Now let's present our first identity:

Proposition 5.2 (Pythagorean Identity). $\sin^2 x + \cos^2 x = 1$ *for* $0 < x < \frac{\pi}{2}$.

Exercise 5.3. Prove the Pythagorean Identity. **Hint:** There's a reason it's called the Pythagorean Identity.

Exercise 5.4. Also prove that $\tan^2 x + 1 = \sec^2 x$ and $\cot^2 x + 1 = \csc^2 x$.

In fact, using this identity along with some algebraic manipulations, we can actually already solve some easy and middle difficulty AIME problems:

Example 5.5 (2003 AIME I #4). Given that $\log_{10}(\sin x) + \log_{10}(\cos x) = -1$ and that $\log_{10}(\sin x + \cos x) = \frac{1}{2}(\log_{10} n - 1)$, find n.

Solution. Immediately, it appears that the equations can be simplified and somehow combined because the log parts share a common base. First, combine $\log_{10}(\sin x) + \log_{10}(\cos x)$ in the first equation to get $\log_{10}(\sin x \cos x) = -1$. Exponentiating both sides with base 10, we get

$$\sin x \cos x = \frac{1}{10} \tag{5.1}$$

Simplifying the second equation,

$$\log_{10}(\sin x + \cos x) = \frac{1}{2}(\log_{10} \frac{n}{10})$$
$$\log_{10}(\sin x + \cos x) = (\log_{10} \sqrt{\frac{n}{10}})$$

Exponentiating both sides with base 10, we get

$$\sin x + \cos x = \sqrt{\frac{n}{10}} \tag{5.2}$$

Square both sides, apply the Pythagorean Identity, and substitute equation 5.1 in.

$$\sin^2 x + \cos^2 x + 2\cos x \sin x = \frac{n}{10}$$
$$1 + 2\left(\frac{1}{10}\right) = \frac{n}{10}$$

Thus, $n = 12$. ■

> *Remark.* Squaring some form of $\sin x + \cos x$ then replacing the $\sin^2 x + \cos^2 x$ part with 1 is a common trick that appears on problems involving trig.

> **Example 5.6** (1991 AIME I #9). Suppose that $\sec x + \tan x = \frac{22}{7}$ and that $\csc x + \cot x = \frac{m}{n}$, where $\frac{m}{n}$ is in lowest terms. Find $m + n$.

Solution. Looking at $\sec x + \tan x$ and $\csc x + \cot x$, we notice that they bear a tiny bit of resemblance to the identities $\tan^2 x + 1 = \sec^2 x$ and $\cot^2 x + 1 = \csc^2 x$ that we asked you to prove in a previous exercise.

We wish to have $\tan^2 x$ and $\sec^2 x$ on opposite sides of the equation, so subtract $\sec x$ from both sides of $\sec x + \tan x = \frac{22}{7}$ to get

$$\sec x = \frac{22}{7} - \tan x$$

Then, square both sides and apply the $\tan^2 x + 1 = \sec^2 x$ identity:

$$\sec^2 x = \tan^2 x - 2\left(\frac{22}{7}\right)\tan x + \left(\frac{22}{7}\right)^2$$
$$\sec^2 x + 1 = \tan^2 x + 1 - 2\left(\frac{22}{7}\right)\tan x + \left(\frac{22}{7}\right)^2$$
$$\sec^2 x + 1 = \sec^2 x - 2\left(\frac{22}{7}\right)\tan x + \left(\frac{22}{7}\right)^2$$
$$1 = -2\left(\frac{22}{7}\right)\tan x + \left(\frac{22}{7}\right)^2$$

Thus, $\tan x = \frac{435}{308}$. We then attempt to further simplify the expression $\csc x + \cot x$ in a similar manner so that we get something in terms of $\cot x$. This would be very helpful because $\cot x = \frac{1}{\tan x}$ and we already know the value of $\tan x$. For ease of writing, let $y = \frac{m}{n}$. We use the exact same procedure as before:

$$\csc x = y - \cot x$$
$$\csc^2 x = \cot^2 x - 2y\tan x + y^2$$
$$\csc^2 x + 1 = \cot^2 x + 1 - 2y\cot x + y^2$$
$$1 = -2y\tan x + y^2$$

Substituting in $\cot x = \frac{1}{\tan x} = \frac{308}{435}$ and rearranging, we get

$$0 = y^2 - 2\left(\frac{308}{435}\right)y - 1 \tag{5.3}$$

$$0 = 435y^2 - 2(308)y - 435 \tag{5.4}$$

This quadratic can be solved by factoring it into $(15y - 29)(29y + 15)$ or by the quadratic formula. We now have two solutions, one of which is extraneous. Since the signs of the two solutions differ, it would be nice to find out whether our answer is positive or negative.

Note that we showed that $\tan x = \frac{435}{308}$, which is positive. Since $\tan x = \frac{\sin x}{\cos x}$, $\sin x$ and $\cos x$ are either both positive or both negative.

Another useful equation is the given one, $\sec x + \tan x = \frac{22}{7}$. We can rewrite this as

$$\begin{aligned} \sec x + \tan x &= \frac{22}{7} \\ \frac{1}{\cos x} + \frac{\sin x}{\cos x} &= \frac{22}{7} \\ \frac{1 + \sin x}{\cos x} &= \frac{22}{7}. \end{aligned}$$

Note that $1 + \sin x$ is always nonnegative, meaning that $\cos x$ is positive. Therefore, both $\sin x$ and $\cos x$ are positive.

Since $\sin x, \cos x$ are positive, we must have that $\csc x + \cot x$ is positive, so $y = \frac{29}{15}$ and not $-\frac{15}{29}$. Our answer is $m + n = 29 + 15 = 44$. ■

Example 5.7 (2019 AIME I #8). Let x be a real number such that $\sin^{10} x + \cos^{10} x = \frac{11}{36}$. Then $\sin^{12} x + \cos^{12} x = \frac{m}{n}$ where m and n are relatively prime positive integers. Find $m + n$.

Solution. Substitute $a = \sin^2 x$ and $b = \cos^2 x$. (This is a natural choice because all the exponents are even). Note that we have $a + b = 1$ by the Pythagorean Identity as well as $a^5 + b^5 = \frac{11}{36}$ from the problem statement.

Then we can substitute in $b = 1 - a$ to get

$$a^5 + (1 - a)^5 = \frac{11}{36}.$$

Expanding out the left side can be made easier by substituting $c = 1/2 - a$ as this will cancel out the odd-powered terms by symmetry. Performing this substitution and expanding gives

$$\begin{aligned} \frac{11}{36} &= \left(\frac{1}{2} - c\right)^5 + \left(\frac{1}{2} + c\right)^5 \\ &= \frac{1}{16}(80c^4 + 40c^2 + 1). \end{aligned}$$

Now we can use the quadratic formula or factor (note that the equation is a quadratic in c^2) to get $c^2 = \frac{1}{12}$. This gives $c = \pm\frac{1}{2\sqrt{3}}$. We can choose either the positive or negative value of c. We want the value of

$$a^6 + (1 - a)^6 = \left(\frac{1}{2} - c\right)^6 + \left(\frac{1}{2} + c\right)^6.$$

Some computation (made easier with difference of cubes) gives us a value of $\frac{13}{54}$, so our answer is $13 + 54 = 67$.

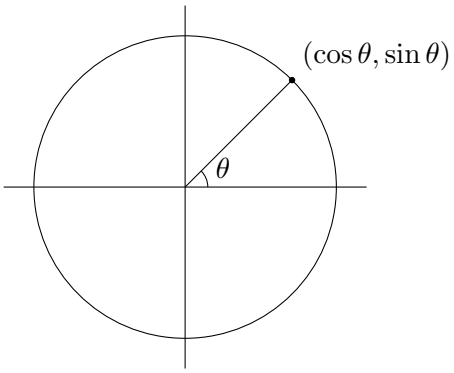
■

Notice that in our solution, we pretty much used no geometry, even though the trigonometric functions are defined geometrically! This is actually pretty much true of almost all problems that explicitly state trig functions: algebraic manipulation and gratuitous usage of identities are usually your best bets, and geometric insights are rarely necessary or even useful.

> *Remark.* In fact, it's even common practice in computational geometry to blindly use the Law of Cosines and Law of Sines to reduce problems to pure algebra, which is really the true power of trigonometry. We'll cover these two theorems in Week 3 when we do geometry.

§5.2 The Unit Circle

It turns out that there's a generalized definition of the trigonometric identities. The idea is to consider the circle $x^2 + y^2 = 1$ plotted on the Cartesian plane; if we take an arbitrary point (x_1, y_1) on this circle, then if θ is the counterclockwise angle made by the line between $(0, 0)$ and (x_1, y_1) and the x-axis, we can define $\cos\theta = x_1$ and $\sin\theta = y_1$. Similar definitions hold for the other trig functions; for instance, $\tan\theta = \frac{y_1}{x_1}$.



This might seem a little confusing. What do we do with negative angles, or angles greater than or equal to 2π?.

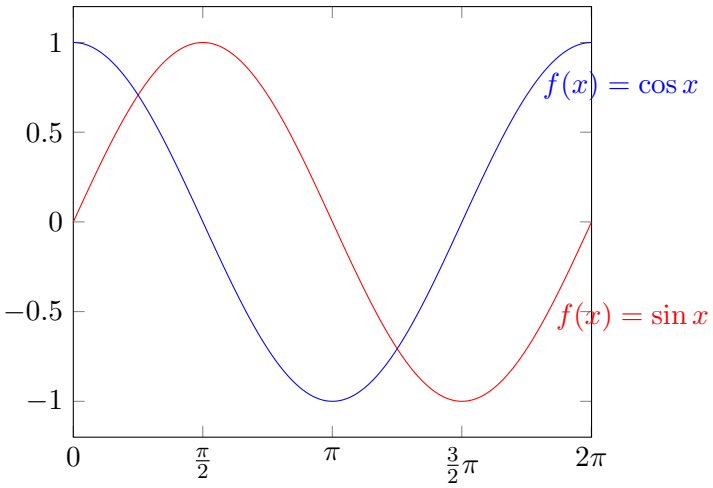
The key is to note that 2π is a full rotation around the unit circle, so $\cos(2\pi) = \cos(0) = 1$ and $\sin(2\pi) = \sin(0) = 0$, and the same is true for any multiple of 2π.

This means that the sine and cosine of an angle θ are equal to the sine and cosine of θ modulo 2π, respectively, so sine and cosine are **periodic functions**: they take all of their possible values in a fixed interval, $[0, 2\pi)$, and then repeat themselves from $[2\pi, 4\pi), [4\pi, 8\pi]$, and so on to infinity. Thus, we say that sin has period 2π, or sin is periodic modulo 2π.

We can interpret negative angles as clockwise angles instead; therefore, an argument of $-\frac{3\pi}{2}$ inputted to the sine and cosine functions would return the same outputs as an argument of $\frac{\pi}{2}$.

That way, the intervals also repeat to the left: the values of $[0, 2\pi]$ are repeated in the intervals $[-2\pi, 0], [-4\pi, -2\pi)$, etc. This also implies that sine is an **odd** function and that cosine is an **even** function; that is, $\sin(-x) = -\sin(x)$ for all real x and $\cos(-x) = \cos(x)$ for all real x.

Here's a graph of $\sin x$ and $\cos x$:



Exercise 5.8. Show that tan is periodic modulo π, and try graphing the function.

Exercise 5.9. Find $\cos(\frac{\pi}{2})$ and $\cos(\frac{5\pi}{3})$.

Note that the sine graph is actually the cosine graph shifted by $\frac{\pi}{2}$ because of our earlier observation that $\sin x = \cos(\frac{\pi}{2} - x)$. It's also useful to note that $\sin x = \sin(\pi - x)$ along with $\cos x = -\cos(\pi - x)$. Applying these can often come in handy with making an expression in terms of sines or cosines only, as we will see in the next example.

Example 5.10. Find the value of

$$\tan\frac{\pi}{20}\tan\frac{\pi}{10}\tan\frac{3\pi}{20}\tan\frac{\pi}{5}\dots\tan\frac{9\pi}{20}.$$

Solution. Let's try putting everything in terms of sines and cosines; this is often a useful strategy if nothing clever comes to mind. The expression is equal to

$$\frac{\sin\frac{\pi}{20}\sin\frac{2\pi}{20}\sin\frac{3\pi}{20}\sin\frac{4\pi}{20}\dots\sin\frac{9\pi}{20}}{\cos\frac{\pi}{20}\cos\frac{2\pi}{20}\cos\frac{3\pi}{20}\cos\frac{4\pi}{20}\dots\cos\frac{9\pi}{20}},$$

but $\cos(x) = \sin(\frac{\pi}{2} - x)$, so the expression becomes

$$\frac{\sin\frac{\pi}{20}\sin\frac{2\pi}{20}\sin\frac{3\pi}{20}\sin\frac{4\pi}{20}\dots\sin\frac{9\pi}{20}}{\sin\frac{9\pi}{20}\sin\frac{8\pi}{20}\sin\frac{7\pi}{20}\sin\frac{6\pi}{20}\dots\sin\frac{\pi}{20}} = 1.$$

■

Now we can present some more identities:

Proposition 5.11 (Angle Addition Identities). *For real x, y, we have*

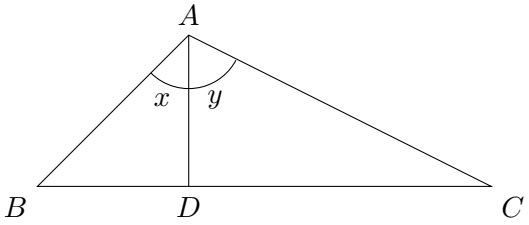
$$\sin(x+y) = \sin x\cos y + \sin y\cos x$$

$$\cos(x+y) = \cos x\cos y - \sin y\sin x$$

Proof. We first show the sine Angle Addition Identity; we will only really prove the identity for the case $0 < x + y < \pi$. The cases where $\pi < x + y < 2\pi$ or $x + y = 0, \pi$ are left as an exercise.

Consider a triangle $\triangle ABC$ with largest angle at $\angle A$. Let D be the foot of the altitude from A to BC, and let $x = \angle BAD$ and $y = \angle CAD$. Then we must have

$$\begin{aligned}
[ABC] &= [ABD] + [ACD] \\
\frac{AB \cdot AC \sin(x+y)}{2} &= \frac{AD \cdot BD}{2} + \frac{AD \cdot CD}{2} \\
\frac{\frac{1}{\cos x \cdot \frac{1}{\cos y}\sin(x+y)}}{2} &= \frac{AB \cdot \cos x \cdot AB \cdot \sin x}{2} + \frac{AC \cdot \cos y \cdot AC \cdot \sin y}{2} \\
\frac{\sin(x+y)}{\cos x \cos y} &= \frac{\sin x}{\cos x} + \frac{\sin y}{\cos y} \\
\sin(x+y) &= \sin x \cos y + \sin y \cos x.
\end{aligned}$$



Now we show the cosine Angle Addition Identity, which this time requires no geometry and as a result will be proven for all real x, y. We mentioned earlier that $\cos(\frac{\pi}{2} - x) = \sin x$, so

$$\begin{aligned}
\cos(x+y) &= \sin\left(\frac{\pi}{2} - x - y\right) \\
&= \sin\left(\frac{\pi}{2} - x\right)\cos(-y) + \sin(-y)\cos\left(\frac{\pi}{2} - x\right) \\
&= \cos x \cos y - \sin x \sin y
\end{aligned}$$

as desired. ■

Exercise 5.12. Prove the sine Angle Addition Identity for the cases not shown above without using geometry.

These are probably the most important trig identities you need to know. From them, we can quickly derive a host of new identities:

Proposition 5.13 (Angle Subtraction Identities). *We have*

$$\sin(x-y) = \sin x \cos y - \sin y \cos x$$

$$\cos(x-y) = \cos x \cos y + \sin x \sin y$$

for real x, y.

Proposition 5.14 (Double Angle Identities). *We have*

$$\sin(2x) = 2 \sin x \cos y$$

$$\begin{aligned}\cos(2x) &= \cos^2 x - \sin^2 x \\ &= 1 - 2\sin^2 x \\ &= 2\cos^2 x - 1.\end{aligned}$$

for real x.

Proposition 5.15 (Half Angle Identities). *We have*

$$\sin\left(\frac{x}{2}\right) = \pm\sqrt{\frac{1-\cos x}{2}}$$

$$\cos\left(\frac{x}{2}\right) = \pm\sqrt{\frac{1+\cos x}{2}}$$

for real x. Of course, $\cos(\frac{x}{2})$ and $\sin(\frac{x}{2})$ do not actually take on two values, and the sign is dependent upon which quadrant the angle $\frac{x}{2}$ is in.

Proposition 5.16 (Product-to-sum Identities). *We have*

$$\sin x \sin y = \frac{1}{2}(\sin(x+y) + \cos(x-y))$$

$$\cos x \cos y = \frac{1}{2}(\cos(x+y) + \cos(x-y))$$

for real x, y.

Proposition 5.17 (Sum-to-product Identities). *We have*

$$\sin x + \sin y = 2\sin\left(\frac{x+y}{2}\right)\cos\left(\frac{x-y}{2}\right)$$

$$\cos x + \cos y = 2\cos\left(\frac{x+y}{2}\right)\cos\left(\frac{x-y}{2}\right)$$

for real x, y.

Exercise 5.18. Derive these identities yourself. **Hint:** The Pythagorean Identity is useful for the cosine Double Angle Identity, and the Double Angle Identities are useful for the Half Angle Identities. Use the Angle Addition Identities to prove the Product-to-sum Identities, and then make a substitution into the Product-to-sum Identities to get the Sum-to-product Identities.

Exercise 5.19. Prove that $\tan(x+y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}$ for real x, y.

Exercise 5.20. Show that $\sin(\frac{\pi}{12}) = \frac{\sqrt{6}-\sqrt{2}}{4}$.

Example 5.21 (2012 AIME II #9). Let x and y be real numbers such that $\frac{\sin x}{\sin y} = 3$ and $\frac{\cos x}{\cos y} = \frac{1}{2}$. The value of $\frac{\sin 2x}{\sin 2y} + \frac{\cos 2x}{\cos 2y}$ can be expressed in the form $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p+q$.

Solution. To find $\frac{\sin 2x}{\sin 2y}$, we can just observe by the sine Double Angle Formula that this is equal to

$$\frac{2\sin x\cos x}{2\sin y\cos y} = \frac{3}{2}.$$

That was pretty quick, but unfortunately $\frac{\cos 2x}{\cos 2y}$ isn't as easy. Let's try to get rid of one variable.

We'll start with x first because $\frac{1}{2}$ is nicer to deal with than $\frac{1}{3}$. Since $\sin x = 3\sin y$ and $\cos x = \frac{1}{2}\cos y$, we can use the Pythagorean Identity to get

$$1 = \sin^2 x + \cos^2 x = 9\sin^2 y + \frac{1}{4}\cos^2 y = 9\sin^2 y + \frac{1}{4}(1-\sin^2 y).$$

Solving for $\sin^2 y$, we get $\frac{3}{35}$. Now we can plug and chug with the cosine Double Angle Formula: we get

$$\cos 2x = 1 - 2\sin^2 x = 1 - 18\sin^2 y = 1 - \frac{54}{35} = -\frac{19}{35}$$

and

$$\cos 2y = 1 - 2\sin^2 y = 1 - \frac{6}{35} = \frac{29}{35},$$

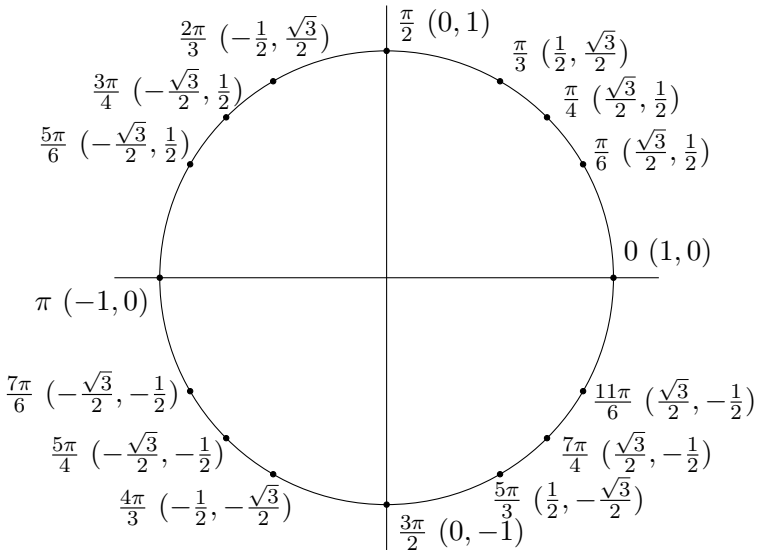
so we get

$$\frac{\sin 2x}{\sin 2y} + \frac{\cos 2x}{\cos 2y} = \frac{3}{2} - \frac{19}{29} = \frac{49}{58}$$

so our final answer is $p + q = 107$. ■

We'll end this section with a list of the values of trigonometric functions of some common angles, which is definitely worth memorizing.

Angle	sin	cos	tan
0	0	1	0
$\frac{\pi}{6}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{3}$
$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1
$\frac{\pi}{3}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$\sqrt{3}$
$\frac{\pi}{2}$	1	0	undefined
$\frac{2\pi}{3}$	$\frac{\sqrt{3}}{2}$	$-\frac{1}{2}$	$-\sqrt{3}$
$\frac{3\pi}{4}$	$\frac{\sqrt{2}}{2}$	$-\frac{\sqrt{2}}{2}$	-1
$\frac{5\pi}{6}$	$\frac{1}{2}$	$-\frac{\sqrt{3}}{2}$	$-\frac{\sqrt{3}}{3}$
π	0	-1	0
$\frac{7\pi}{6}$	$-\frac{1}{2}$	$-\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{3}$
$\frac{5\pi}{4}$	$-\frac{\sqrt{2}}{2}$	$-\frac{\sqrt{2}}{2}$	1
$\frac{4\pi}{3}$	$-\frac{\sqrt{3}}{2}$	$-\frac{1}{2}$	$\sqrt{3}$
$\frac{3\pi}{2}$	-1	0	undefined
$\frac{5\pi}{3}$	$-\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$-\sqrt{3}$
$\frac{7\pi}{4}$	$-\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	-1
$\frac{11\pi}{6}$	$-\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$-\frac{\sqrt{3}}{3}$
2π	0	1	0



A nice trick to remember these values is to learn the first quadrant and then use the mnemonic **A**ll **S**tudents **T**ake **C**alculus to figure out the signs: **A**ll the trig functions are positive in the first quadrant, only **S**ine is positive in the second quadrant, only **T**angent is positive in the third quadrant, and only **C**osine is positive in the fourth quadrant.

Example 5.22 (2000 AIME II #15). Find the least positive integer n such that

$$\frac{1}{\sin 45^\circ \sin 46^\circ} + \frac{1}{\sin 47^\circ \sin 48^\circ} + \ldots + \frac{1}{\sin 133^\circ \sin 134^\circ} = \frac{1}{\sin n^\circ}.$$

Solution. Whenever we see a long fraction summation equal to a nice result, telescoping should be the first thing that comes to mind. Let's keep this in mind.

We can observe that the 1 in the numerator on the right hand side is sort of suspicious. This means that multiplying both sides by something nice is probably going to be useful. Now here comes the intuitive leap: multiplying by $\sin 1^\circ$ gives us what we want. Why is this true?

Well, $\sin 1^\circ = \sin((x+1)^\circ - x^\circ) = \sin(x+1)^\circ \cos x^\circ - \sin x^\circ \cos(x+1)^\circ$, and this leads to nice cancellation both in the fractions and of terms using the fact that $\cot(x) = -\cot(\pi - x)$:

$$\begin{aligned}
\frac{\sin 1^\circ}{\sin n^\circ} &= \frac{\sin 1^\circ}{\sin 45^\circ \sin 46^\circ} + \frac{\sin 1^\circ}{\sin 47^\circ \sin 48^\circ} + \ldots + \frac{\sin 1^\circ}{\sin 133^\circ \sin 134^\circ} \\
&= \frac{\sin 46^\circ \cos 45^\circ - \sin 45^\circ \cos 46^\circ}{\sin 45^\circ \sin 46^\circ} + \ldots + \frac{\sin 134^\circ \cos 133^\circ - \sin 133^\circ \cos 134^\circ}{\sin 133^\circ \sin 134^\circ} \\
&= (\cot 45^\circ - \cot 46^\circ) + (\cot 47^\circ - \cot 48^\circ) + \ldots + (\cot 133^\circ - \cot 134^\circ) \\
&= \cot 45^\circ - (\cot 46^\circ + \cot 134^\circ) + (\cot 47^\circ + \cot 133^\circ) + \ldots + (\cot 89^\circ - \cot 91^\circ) \\
&= \cot 45^\circ \\
&= 1,
\end{aligned}$$

so $n = 1$ clearly works. ■

§5.3 Complex Numbers

Say we have the following problem:

Proposition 5.23. *Solve the equation* $x^2 + 1 = 0$.

This seems ludicrous– we'd need the square root of -1. What is $\sqrt{-1}$? It can't be any of the numbers we're familiar with, because whenever we take the square of a number it's non-negative. This motivates the idea of **complex numbers**.

An **imaginary number** is defined as any number whose square is negative. We define $i = \sqrt{-1}$ as the **imaginary unit**.. In order to distinguish between pure imaginary numbers and the numbers we're familiar with, we call the numbers that we normally work with **real numbers**, which are numbers whose square is a non-negative value. Note that this means any imaginary number a can be written in the form $b \cdot i$, where b is a real number and i is the imaginary unit.

Example 5.24. Solve $x^2 + 4$.

Solution. Note that $x^2 = -4 \implies x = \sqrt{-4} = \sqrt{-1} \cdot \sqrt{4} = \pm 2i$. ■

Example 5.25. What is the value of $9i \cdot 4i$?

Solution.

$$9i \cdot 4i = 9 \cdot 4 \cdot i^2 = 9 \cdot 4 \cdot -1 = -36$$

■

Exercise 5.26. Find the values of $i^3, -\frac{1}{i}$, and i^7.

Where have we discussed taking the square root of a negative number before? When talking about quadratics, we mentioned that the discriminant must be non-negative in order for there to be a solution. Now we have a way to solve it when it's negative!

Example 5.27. Solve the equation $x^2 + x + 1 = 0$.

Solution. We use the quadratic formula:

$$x = \frac{-1 \pm \sqrt{1^2 - 4 \cdot 1 \cdot 1}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}i}{2}$$

■

Some of you may notice that we have actually added together a pure imaginary number and real number: note that if we square it, it's neither a non-negative nor negative real number. In fact, it's another real number plus an imaginary number! We call this number a **complex number**, or the sum between a real number and imaginary number. Remembering that we can look at imaginary numbers as a real number multiplied by i, we can characterize complex numbers as follows:

Definition 5.28. A *complex number* is a number in the form $a + bi$, where a and b are real and i is the imaginary unit.

We refer to a and b as the **real part** and **imaginary part** of a complex number $a + bi$, respectively. For a complex number z, we usually denote the real part as $\Re(z)$ and the imaginary part as $\Im(z)$. Note that both $\Re(z)$ and $\Im(z)$ both return real numbers. One seemingly trivial but nonetheless important idea to keep in mind is the following:

Proposition 5.29. *Two complex numbers x and y are equal if and only if their real parts are equal and their imaginary parts are equal.*

This should be fairly intuitive. Let's see how we can use this fact:

Example 5.30. If $a^2 + 4i = 25 - bi$, where a and b are real numbers, then find all possible pairs (a, b).

Solution. Remember two complex numbers are equal if and only if their real and imaginary parts match up with each other. This gives us the equations

$$a^2 = 25, 4 = -b$$

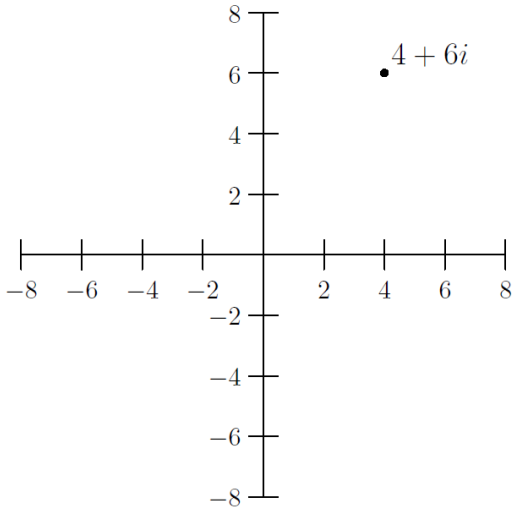
which imply the only solutions are $(a, b) = (\pm 5, -4)$. ■

Exercise 5.31. Determine which of the following are complex numbers: i, $1 - 2i$, $3/\pi$.

Exercise 5.32. Express the quotient $(a + bi)/(c + di)$ in the form $p + qi$.

§5.4 The Complex Plane

We're accustomed to graphing real numbers on a number line, but what if we tried to extend this to complex numbers? We'd probably want to keep the real and imaginary parts separate; this means that we should have two axes, similar to the xy-plane. This leads to the idea of the **complex plane**. If we wanted to graph the complex number $a + bi$ in the complex plane, then the "x-coordinate" would be a and the "y-coordinate" would be b; that is, the x-axis is the **real axis** and the y-axis is the **imaginary axis**. The origin is still $(0, 0)$, which corresponds to the complex number 0.



Definition 5.33. The **magnitude** of a complex number $z = a + bi$ is the distance from the origin, or $\sqrt{a^2 + b^2}$. The magnitude of z is denoted as $|z|$, since if z is real then this is equivalent to the absolute value function.

Exercise 5.34. Show that for any complex numbers z and w, $|zw| = |z||w|$.

Definition 5.35. the **conjugate** of a complex number $z = a + bi$ is defined as $a - bi$. The conjugate of z is denoted as $\overline{z}$.

Exercise 5.36. Show that for any complex numbers z and w, $\overline{\overline{z}} = z$, $\overline{z + w} = \overline{z} + \overline{w}$, and $\overline{zw} = \overline{z} \cdot \overline{w}$.

Exercise 5.37. Show that a complex number z is real if and only if $z = \overline{z}$, and that it is imaginary if and only if $z = -\overline{z}$.

Exercise 5.38. Show that $z\overline{z} = |z|^2$.

Exercise 5.39. Graphically, what does the conjugate of z represent?

Arithmetic is also doable on the complex plane. For addition, it's quite simple to apply our knowledge. If we have points $a+bi$ and $c+di$, then the sum is just $(a+c)+(b+d)i$. Multiplying $a + bi$ by a real c is also very simple as we are given $c(a + bi)$. However, multiplication of two complex numbers is slightly more unwieldy in this form, but thankfully this is remedied in the following section.

§5.5 Euler's Formula

Before we introduce Euler's Formula, we introduce some new material.

Consider a complex number $z = a + bi$. First, let's divide $a + bi$ by a real number c such that $\frac{a+bi}{c}$ has a distance of 1 from the origin; this puts z on the unit circle.

Then, it follows from our generalized definitions of sine and cosine that if θ is the measure of the counterclockwise angle made by the line between $a + bi$ and 0 and the real axis (called $a + bi$'s **argument**), $\frac{a}{c}$ can be described as $\cos\theta$ and $\frac{b}{c}$ can be described as $\sin\theta$.

Therefore, $\frac{a+bi}{c}$ is equal to $\cos\theta + i\sin\theta$, and multiplying by c, we have that

$$a + bi = c\cos\theta + ic\sin\theta.$$

This is a very important interpretation of the complex numbers known as **polar form**, because we're expressing z in terms of an argument and a magnitude only, which is exactly what regular polar coordinates are in the Cartesian plane. The representation $a+bi$ is known as **rectangular form** because $a + bi$, a, bi, and 0 are the vertices of a rectangle.

Notation. Let $\cos\theta + i\sin\theta = \operatorname{cis}\theta$.

We first introduce an important theorem that will help us with Euler's Formula.

Theorem 5.40 (De Moivre's Theorem). *$\operatorname{cis} n\theta = \operatorname{cis}^n\theta$ for all integral n and real θ.*

Proof. To prove this for all integral n, we use induction. Fix θ. First, we know that $\operatorname{cis}(0 \cdot \theta) = \operatorname{cis} 0 = \cos 0 + i\sin 0 = 1 = \operatorname{cis}^0\theta$, so our base case is complete.

We assume that this the assertion is true for some nonnegative integer k, and we prove it for $k+1$. It follows that

$$\begin{aligned}
&(\cos\theta + i\sin\theta)^{k+1} = (\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)^k \\
\implies &(\cos\theta + i\sin\theta)^{k+1} = (\cos\theta + i\sin\theta)(\cos k\theta + i\sin k\theta) \text{ from our assumption for } k \\
\implies &(\cos\theta + i\sin\theta)^{k+1} = \cos\theta\cos k\theta + i\cos\theta\sin k\theta + i\sin\theta\cos k\theta - \sin\theta\sin k\theta \\
\implies &(\cos\theta + i\sin\theta)^{k+1} = \cos((k+1)\theta) + i\sin((k+1)\theta)
\end{aligned}$$

from our angle addition identities.

Hence, we are done as we've proven the base case and the inductive step. To extend the statement to negative integers as well, observe that $\operatorname{cis}\theta$ is the conjugate of $\operatorname{cis}(-\theta)$, so $\operatorname{cis}\theta\operatorname{cis}(-\theta) = 1 \implies \operatorname{cis}(-\theta) = \operatorname{cis}^{-1}\theta$. Thus, for arbitrary n, $\operatorname{cis}(-n\theta) = (\operatorname{cis}(-\theta))^n = (\operatorname{cis}^{-1}(\theta))^n = \operatorname{cis}^{-n}\theta$ as desired. ■

Exercise 5.41. Prove that $\sin 3x = (4\cos^2 x - 1)\sin x$.

With De Moivre, we can now understand Euler's formula. We state Euler's formula without proof since the proof requires calculus, which is out of the scope of this class.

Theorem 5.42 (Euler's Formula)**.** *$e^{ix} = \operatorname{cis} x$ for all real x.*

This third form is called **exponential form** for obvious reasons. Notice that this gives us a very natural explanation of de Moivre, and also allows us to understand the consequences of **multiplying complex numbers** much more easily:

Proposition 5.43. *We have*

$$\operatorname{cis} x \operatorname{cis} y = \operatorname{cis}(x+y),$$
$$\frac{\operatorname{cis} x}{\operatorname{cis} y} = \operatorname{cis}(x-y)$$

for real x, y.

This is much faster than multiplying complex numbers in rectangular form!

Try to digest the graphical significance of these facts. If we multiply a complex number by $\operatorname{cis}\theta$, then we just rotate it in the complex plane by θ. So multiplication by any complex number just corresponds to scaling by the magnitude, then rotating by the argument.

Exercise 5.44. Prove Proposition 5.43.

From Euler's Formula, we get the beautiful relation known as Euler's Identity:

Theorem 5.45. *(Euler's Identity) $e^{i\pi} + 1 = 0$.*

Proof. $e^{i\pi} = \operatorname{cis}\pi = \cos\pi + i\sin\pi = -1 \iff e^{i\pi} + 1 = 0$ ■

The following example demonstrates the power of Euler's Formula:

Example 5.46. (Mu Alpha Theta 1991) Evaluate

$$\sum_{n=0}^{\infty} \frac{\cos(n\theta)}{2^n}$$

where $\cos\theta = \frac{1}{5}$.

Solution. First, let's try to see why Euler's Formula is a good candidate for this problem.

The key here is that the problem asks us to deal with the cosine of multiples of a fixed angle. We know that we can easily deal with multiples of angles from De Moivre's Theorem, so we want to tie this in somehow.

Moreover, we have a sum that resembles a geometric sum, except we have $\cos(n\theta)$ in the numerator— then we want to use something that ties in De Moivre's Theorem and geometric series together, which is exactly what Euler's Formula does!

So how will we apply Euler's Formula? Well, the key idea is that $\cos(n\theta)$ is the *real part* of $e^{i(n\theta)}$. Why? Well, this is immediate by Euler's Formula:

$$e^{i(n\theta)} = \cos(n\theta) + i\sin(n\theta)$$

Thus, our problem is equivalent to summing the real parts of $\frac{e^{i(n\theta)}}{2^n}$, or the real part of the sum

$$\sum_{n=0}^{\infty} \frac{e^{i(n\theta)}}{2^n}$$

Now we have ourselves a geometric series, with first term $\frac{e^0}{2^0} = 1$ and ratio $\frac{e^{i\theta}}{2}$. We can evaluate the sum with techniques we already know:

$$\sum_{n=0}^{\infty} \frac{e^{i(n\theta)}}{2^n} = \frac{1}{1-\frac{e^{i\theta}}{2}} = \frac{2}{2-e^{i\theta}}$$

From the Pythagorean Identity, we have $\cos^2\theta + \sin^2\theta = 1$. Plugging in $\cos\theta$, we get $\sin\theta = \pm\frac{2\sqrt{6}}{5}$. How do we know which one to use? The answer is that we don't— the problem doesn't specify which quadrant θ lies in. However, remember that we only care about the real part of the sum, or just the cosines. Since taking plus or minus doesn't affect the cosines, we can just choose any value to use! Let's take the positive value; from Euler's Formula,

$$e^{i\theta} = \cos\theta + i\sin\theta = \frac{1}{5} + \frac{2\sqrt{6}}{5}i$$

Plugging this into our sum,

$$\frac{2}{2-e^{i\theta}} = \frac{2}{2-\left(\frac{1}{5}+\frac{2\sqrt{6}}{5}i\right)} = \frac{2}{\frac{9}{5}+\frac{2\sqrt{6}}{5}i}$$

Exercise 5.47. Evaluate the sum: although it's tedious, it's important to practice rationalizing the denominator so that you can do it faster later on.

As we alluded to in the exercise, we can simply rationalize the denominator:

$$\frac{2}{\frac{9}{5}+\frac{2\sqrt{6}}{5}i} = \frac{2\left(\frac{9}{5}-\frac{2\sqrt{6}}{5}i\right)}{\left(\frac{9}{5}+\frac{2\sqrt{6}}{5}i\right)\left(\frac{9}{5}-\frac{2\sqrt{6}}{5}i\right)} = \frac{\frac{18}{5}-\frac{4\sqrt{6}}{5}i}{\frac{81+24}{25}}$$

Since we just want the real part, our answer is

$$\frac{\frac{18}{5}}{\frac{105}{25}} = \frac{90}{105} = \frac{6}{7}$$

■

Let's recap the steps we took again. First, we noticed that the problem involved the cosine of multiples of a fixed angle, θ, so that told us we should use De Moivre's and complex numbers somehow. Combining this with the fact that we had a 2^n, we decided that geometric series was the way to go, which led to using Euler's Formula, since it gives us an exponential form of complex numbers. From here, we knew that we could evaluate the series using the geometric series sum formula, and then take the real part to just get the cosines.

Exercise 5.48. Evaluate

$$\sum_{n=0}^{\infty} \frac{\sin(n\theta)}{2^n}$$

where $\cos\theta = \frac{1}{5}$.

Let's look at another application of De Moivre's Theorem and Euler's Formula:

Theorem 5.49. *The solutions to the equation $x^n = 1$ for some natural number n are of the form $e^{i\frac{2\pi k}{n}}$, where $0 \le k \le n$.*

Proof. Suppose the complex number $z = re^{i\theta}$ is a root of $x^n - 1$. Since r is the magnitude of z, the magnitude of z^n must be r^n. Since r is a positive real number and $r^n = 1$, we must have $r = 1$. Thus, $z = e^{i\theta}$. We need $z^n = e^{in\theta}$ to equal 1. Note that $e^{i2\pi} = \cos(2\pi) + i\sin 2\pi = 1$, so

$$e^{in\theta} = e^{i2\pi k} = 1$$

for some positive k.

By exponent rules, we must have $n\theta = 2\pi k \implies \theta = \frac{2\pi k}{n}$. Now, if $k \ge n$, we can pull out $e^{2\pi}$, which is equal to one, so it is a duplicate of one of the roots with $0 \le k \le n$. The same goes for the other direction: if $k < 0$, then we can multiply by $e^{2\pi} = 1$ to get one of the roots already described.

Thus, $e^{\frac{i2\pi k}{n}}$ for $0 \le k \le n$ characterizes the n distinct roots of the polynomial $x^n - 1$ (note that this also satisfies the Fundamental Theorem of Algebra). ■

These n roots are known as the nth roots of unity. Note that the angle between each consecutive root of unity is constant, and the magnitude is always 1, so geometrically, they form a regular n-gon in the complex plane.

Here's an example of this in action:

Example 5.50 (2014 AIME II, Modified). Let z be a complex number and P be the polygon in the complex plane whose vertices are z and every w such that $\frac{1}{z+w} = \frac{1}{z} + \frac{1}{w}$. What geometric shape is P?

Solution. Let's first interpret the given condition on z and w. Combining the fractions and rearranging, we get

$$\frac{1}{z+w} = \frac{1}{z} + \frac{1}{w} = \frac{z+w}{zw} \implies (z+w)^2 = zw$$

which means $z^2+zw+w^2=0$. But wait! This expression is a factor of difference of cubes. We can rewrite our equation, then, in the following form:

$$z^2+zw+w^2=\frac{z^3-w^3}{z-w}=0$$

This means that the solutions for z are the solutions of $z^3-w^3=0$ and $z\neq w$. Since z is nonzero, w is nonzero, so we can divide the equation by z^3:

$$z^3-w^3=0 \implies 1-\left(\frac{w}{z}\right)^3=0$$

As we talked about earlier, this means that $\frac{w}{z}$ are the 3rd roots of unity, except for 1, since it got discarded.

We want the area formed by all possible points w and z in the complex plane, so let's interpret our points geometrically. We have two values of w since z is fixed and $\frac{w}{z}$ is a third root of unity other than 1. If ω is a third root of unity other than 1 (e.g. $\operatorname{cis}\frac{2\pi}{3}$), then ω^2 is the other third root of unity not equal to 1 (you can check this yourself).

Then, letting $\omega=\frac{w}{z}$, we get that our three vertices are z, zw, and zw^2. These are the three third roots of unity, all multiplied by z. What does this mean? The third roots of unity form an equilateral triangle in the complex plane, but do we still have an equilateral triangle in this case?

It turns out we do. If we let $z=|z|\operatorname{cis}\theta$, then multiplication by z simply scales up each vertex by $|z|$ then rotates it by θ. This still preserves the distance between the three points, so our answer is an equilateral triangle. ■

Exercise 5.51. The original problem gives $|z|=2014$ and asks for the area of P. Try solving it.

§5.6 Problems

Problem 5.1 (1988 AHSME)**.** [5] The complex number z satisfies $z+|z|=2+8i$. What is $|z|^2$? Note: if $z=a+bi$, then $|z|=\sqrt{a^2+b^2}$.

Problem 5.2 (2019 AMC 12A)**.** [6] For a certain complex number c, the polynomial

$$P(x)=(x^2-2x+2)(x^2-cx+4)(x^2-4x+8)$$

has exactly 4 distinct roots. What is $|c|^2$?

Problem 5.3 (2019 AMC 12B)**.** [6] How many nonzero complex numbers z have the property that 0, z, and z^3, when represented by points in the complex plane, are the three distinct vertices of an equilateral triangle?

Problem 5.4 (2019 AIME I)**.** [9] Given $f(z)=z^2-19z$, there are complex numbers z with the property that z, $f(z)$, and $f(f(z))$ are the vertices of a right triangle in the complex plane with a right angle at $f(z)$. There are positive integers m and n such that one such value of z is $m+\sqrt{n}+11i$. Find $m+n$.

Problem 5.5 (2018 AIME I)**.** [10] Let N be the number of complex numbers z with the properties that $|z|=1$ and $z^{6!}-z^{5!}$ is a real number. Find the remainder when N is divided by 1000.

Problem 5.6 (2017 AIME I)**.** [8] Let $z_1 = 18 + 83i$, $z_2 = 18 + 39i$, and $z_3 = 78 + 99i$, where $i = \sqrt{-1}$. Let z be the unique complex number with the properties that $\frac{z_3 - z_1}{z_2 - z_1} \cdot \frac{z - z_2}{z - z_3}$ is a real number and the imaginary part of z is the greatest possible. Find the real part of z.

Problem 5.7 (2020 AMC 12A)**.** [10] In the complex plane, let A be the set of solutions to $z^3 - 8 = 0$ and let B be the set of solutions to $z^3 - 8z^2 - 8z + 64 = 0$. We can express the greatest distance between a point of A and a point of B as $a\sqrt{b}$ where a and b are integers and b is not divisible by the square of any integer. What is $a + b$?

Problem 5.8 (2019 AMC 12B)**.** [12] Let $\omega = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$. Let S denote all points in the complex plane of the form $a + b\omega + c\omega^2$, where $0 \le a \le 1, 0 \le b \le 1$, and $0 \le c \le 1$. We can express the area of S as $\frac{p\sqrt{q}}{r}$, where p, q, and r are positive integers. What is $p + q + r$?

Problem 5.9 (2011 AIME II)**.** [10] Let $z_1, z_2, z_3, \ldots, z_{12}$ be the 12 zeroes of the polynomial $z^{12} - 2^{36}$. For each j, let w_j be one of z_j or iz_j. Then the maximum possible value of the real part of $\sum_{j=1}^{12} w_j$ can be written as $m + \sqrt{n}$ where m and n are positive integers. Find $m + n$.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

6 Basic Counting

From a young age, we learn to count. Whether it's the number of fingers on our hands or the toes on our feet, counting is basically an ingrained skill. In this chapter, we will explore the mathematics of counting. This handout will review the basics of counting so we can tackle more advanced concepts in the following days.

§6.1 As Easy As $1, 2, 3$

We first define one of the most common mathematical objects, used almost everywhere.

Definition 6.1. A **set** is an unordered collection of distinct elements (i.e. no repeats). The **cardinality** of a set with a finite number of elements is the number of elements it contains. We denote the cardinality of a set A as $|A|$. We usually use capital letters to represent sets.

Definition 6.2. The **complement** of a set A is the set of all possible elements not in A. The complement is denoted A^C. Context is usually given as to what "all possible elements" means.

> *Remark.* It turns out that there is a way to generalize the definition of cardinality to infinite sets as well. In the process, we end up categorizing different "sizes" of infinities using the so-called **aleph numbers**, and perform arithmetic with them. This is outside of the scope of this handout, but if you're interested, search up "countable sets".

For example, the set S of solutions to the quadratic equation $x^2 - 1 = 0$ is

$$S = \{-1, 1\},$$

and since sets are unordered, this is considered the same set as $\{1, -1\}$.

Sets also aren't limited to just numbers; they can contain anything from words to even other sets. A shorthand we use when describing a set containing all elements satisfying a certain property is with a colon or the symbol $|$. Thus, another way we could describe S is

$$S = \{x : x^2 - 1 = 0\},$$

read as "all x such that x squared minus one equals zero".

Definition 6.3. A **subset** A of a set B is a set such that all of its elements are also elements of B. We denote this by $A \subseteq B$, and if A is not equal to the set B (i.e. there exists an element of B not in A), then we say that A is a **proper subset** of B and denote this by $A \subset B$. The **empty set**, denoted $\emptyset$, is a set containing no elements. Thus, $\emptyset$ is a subset of every set.

Counting problems generally revolve around finding valid subsets, where validity is determined by a given condition in the problem statement.

> **Example 6.4.** How many numbers are in the set $\{1, 2, 3, \ldots, 10\}$?

Solution. You can count the number of terms aloud or write them down and count how many numbers you wrote, but the answer is 10. ■

Obviously, the previous problem wasn't very much of a problem. The numbers were small, and there wasn't much thinking involved at all.

Example 6.5. How many numbers are in $\{101, 102, 103, \ldots, 110\}$? Or $\{5, 6, \ldots, 14\}$?

Solution. The answer is 10 in both these cases. We can figure this out by pairing up numbers with the first 10 integers. In the first case, we pair up each number n with $n+100$: for example, 7 goes to 107. In the second case, we pair up each number n with $n+4$. Thus, both these lists have 10 numbers.

■

Example 6.6. How many numbers are in $\{5, 7, 9 \cdots 39\}$?

Solution. We can match n to $2n+1$. For instance, 1 goes to 5, 2 goes to 7, and so on. Notice that 19 goes to 39. Thus there are 19 numbers in this set. ■

What we just established was a **one-to-one correspondence** between the elements of $\{1, 2, \ldots 10\}$ and the two sets in this problem. Whenever we have a one-to-one correspondence between two sets A and B, we know that $|A| = |B|$. We'll go over this in more detail tomorrow.

Exercise.

(a) Show that if our set is $\{a, a+1, \ldots b\}$ for positive integers $a \leq b$, then the amount of terms in the set is $b - a + 1$.

(b) How many numbers are in the list $2.1, 2.2, \ldots, 4.0$?

§6.2 Constructive Counting

Constructive counting is a fundamental method in combinatorics. Essentially, we count the number of objects that satisfy some property by "constructing" them, i.e. directly creating the possible objects that satisfy the given conditions, and keeping track of how many there are.

Example 6.7. How many ways are there to choose a boy and a girl from a class of 12 boys and 13 girls?

Solution. Note the choice of boys is separate from the choice of girls. Thus, the total number of pairs is $12 \times 13 = 156$. ■

Example 6.8. The Committee of Everaise needs to split 3 unique jobs among 8 staff members. If each staff member can do as many jobs as they please, how many ways are there to assign the jobs?

Solution. Each job can be done by 8 people, and you make a choice for all 3 jobs. Thus the answer is $8 \times 8 \times 8 = 512$. ■

Example 6.9. How many 5 digit integers are there with at least two consecutive 1's?

Solution. Note we have four different places to place the 11: in spots 11___, _11__, __11_, or ___11. However, there's one discrepancy: a five digit integer can't have 0 as its first digit. In the first case, the last three digits can be anything, giving us $10 \times 10 \times 10 = 1000$, but for the last three cases, we only have 9 choices for the first digit, giving us $9 \times 10 \times 10 = 900$. Thus, in total we have $1000 + 3 \times 900 = 3700$. ■

Exercise (2015 AMC8). How many integers between 1000 and 9999 have four distinct digits?

Exercise. Let a *word* be a string of letters that alternate between consonants and vowels. In terms of n, how many *words* of length n are there that start with a consonant? Look at some small specific values of n.

Exercise. A *palindrome* is a word that reads the same forwards and backwards. How many 3-digit palindromes are there? 4-digit? Can you generalize?

§6.3 Casework

Casework is essentially organized constructive counting: we split a problem into several smaller problems (the "cases") with restrictions that make them easier to count, and then we add them up at the end to get the final answer.

Casework can often be very bashy, but on the flip side is useful for solving a huge number of counting problems that appear on the AMC/AIME. One of the most important skills in competition math is to be able to quickly determine whether or not a problem can feasibly be solved with casework within the time limit. This intuition can only be gained through practice.

An important warning is that **cases must be independent**: otherwise, we could potentially count a particular possibility either more than once or not at all (i.e. overcount). Let's take a look at an actual problem:

Example 6.10. (2004 AIME II) A jar has 10 red candies and 10 blue candies. Terry picks two candies at random, then Mary picks two of the remaining candies at random. Given that the probability that they get the same color combination, irrespective of order, is m/n, where m and n are relatively prime positive integers, find $m + n$.

Solution. We first consider the case where Terry picks out 2 red candies. He can pick out 2 red candies with probability

$$\frac{10}{20} \cdot \frac{9}{19} = \frac{9}{38},$$

and the probability that Mary does too after Terry has picked his two red candies is

$$\frac{8}{18} \cdot \frac{7}{17}.$$

Thus, the probability that Mary and Terry both pick two red candies is $\frac{14}{323}$. Next, we count the case where Terry picks out 1 red and 1 blue candy - note that it doesn't matter which order

he picks them due to symmetry, so we just need the second ball to be different. He will pick out this particular combination with

$$\frac{20}{20} \cdot \frac{10}{19}$$

probability and Mary will pick out 1 red and 1 blue with

$$\frac{18}{18} \cdot \frac{9}{17}$$

probability, so the probability that both pick out these combinations is $\frac{90}{323}$. The probability that both pick 2 blue candies is the same as the probability of both picking out 2 red candies, so we just multiply the number we got above by 2 for this last case.

Summing up the probabilities gives

$$\frac{90}{323} + \frac{28}{323} = \frac{118}{323}.$$

■

Let's move onto another example:

Example 6.11. The numbers 1447, 1005, and 1231 have something in common: each is a four-digit number beginning with 1 that has exactly two identical digits. How many such numbers are there?

Solution. Looking at the given examples, we notice two 'types' of integers: one where the 1 is the repeated digit, and the other where a different digit is repeated twice. Hence, this gives us the idea of casework.

Let's look at the case where 1 is the repeated digit. Then, we have 3 places to put the other 1 as we must start with a 1. In the other two spots, we have $9 \cdot 8 = 72$ ways to fill up the other two digits, as they must be distinct from 1, so we have 216 different integers under this case.

For the next case, we again must choose 2 other digits, similarly with 72 different ways. Now, if our digits are x and y, we have 3 ways to arrange them:

$$1xxy$$
$$1xyx$$
$$1yxx$$

so we end up with another 216 different integers. Summing them up gives our answer of $216 + 216 = 432$. ■

Exercise 6.12 (2006 AMC 12A). A bug starts at one vertex of a cube and moves along the edges of the cube according to the following rule. At each vertex the bug will choose to travel along one of the three edges emanating from that vertex. Each edge has equal probability of being chosen, and all choices are independent. What is the probability that after seven moves the bug will have visited every vertex exactly once?

Exercise 6.13 (2005 AMC 10A). How many three-digit numbers satisfy the property that the middle digit is the average of the first and the last digits?

§6.4 Complementary Counting

Casework and constructive counting aren't always the best approaches. There can be times when there are just too many possibilities to consider. But, if we know the total amount of cases, then we can just count the cases that we *don't* want, and then subtract this from the total number of cases to count what we *do* want. You can think of this as taking the complement of a subset.

Example 6.14. How many 4 digit binary strings have at least one 0, assuming a binary string can start with a 0?

Solution. It would be messy to count this directly, as we'd have to keep track of how many 0's there are and their placement in the overall string. However, note there are $2^4 = 16$ total 4 digit binary strings as each string either has 0 or a 1, and there only exists 1 string *without* a 0 (namely, 1111). Thus, there are $16 - 1 = 15$ binary strings with at least one 0.

Putting this in a set perspective, our set was every 4 digit binary string. The condition was having at least one 0, so our original set was split into two subsets: ones with at least one 0 and ones without a 0. ■

Example 6.15. (2006 AMC 10A) How many four-digit positive integers have at least one digit that is a 2 or a 3?

Solution. Again, there's no need to go through all the cases where we have perhaps one 2 no 3s, two 2 and one 3, etc. when we can just count the numbers without a 2 or 3. We have $9 \cdot 10 \cdot 10 \cdot 10 = 9000$ four-digit numbers, and the amount of four-digit integers without a 2 or 3 is $7 \cdot 8 \cdot 8 \cdot 8 = 3584$, so our answer is simply 5416. ■

We will finish off complementary counting with a harder example.

Example 6.16. (2017 AIME II) Find the number of subsets of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ that are subsets of neither $\{1, 2, 3, 4, 5\}$ nor $\{4, 5, 6, 7, 8\}$.

Solution. We first need to have a way to count the number of subsets. If we want to make a subset, either an element from the original set is in the subset or it isn't in it, so this means we have 2^n subsets for a set with n integers.

So, with complementary counting, we want to count the number of subsets that are subsets of $\{1, 2, 3, 4, 5\}$ or $\{4, 5, 6, 7, 8\}$ and subtract them from $2^8 = 256$, the total number of subsets of the original set.

Each set has 5 elements, so each set has 2^5 subsets and combined gives us 64 subsets. However, since $\{4, 5\}$ overlap between the two sets, we inevitably overcount the total number of subsets we need to subtract. Since $\{4, 5\}$ has 4 subsets, our final answer is

$$256 - 64 + 4 = 196.$$

■

Remember that at the end of the day, you still need extensive constructive counting skills to really nail counting problems, but complementary counting is just another strategy to make

your constructive counting more efficient. In general, if you feel that counting the complement involves less cases, you should go for this approach.

Exercise. (2008 AMC 12B) A parking lot has 16 spaces in a row. Twelve cars arrive, each of which requires one parking space, and their drivers chose spaces at random from among the available spaces. Auntie Em then arrives in her SUV, which requires 2 adjacent spaces. What is the probability that she is able to park?

§6.5 Committees

Committees are an extension of constructive counting with a crucial distinction: the order in which the elements are chosen doesn't matter. Through our exploration of committees, we will also investigate binomial coefficients, which are essential for intermediate counting problems and the rest of this week.

Consider the following question:

> **Example 6.17.** How many ways are there to place 5 different books on a bookshelf? Can you find a general formula for the number of ways to place n books?

Solution. We can use constructive counting to solve this problem. There are 5 choices for the first book, 4 for the second, 3 for the third, 2 for the fourth, and 1 remaining book for the fifth. Thus, there are

$$5 \times 4 \times 3 \times 2 \times 1 = 120$$

ways to place the 5 books. For n books, we use the same logic and generalize it. There are n ways to pick the first book, $n-1$ for the second, and so on, until we get to the last book, for which we have 1 choice. Thus, the number of ways to order n books is

$$n \times (n-1) \times (n-2) \cdots 2 \times 1$$

■

Notice that this is the product of all positive integers less than or equal to n. We can use the **factorial** sign, an "!", to denote this. For a positive integer n,

$$n! = n \times (n-1) \times (n-2) \cdots 2 \times 1$$

Note that for all positive integers n, we have $(n+1)! = (n+1) \cdot n!$. Thus, we define 0! to be 1.

Factorials show up very often in counting because $n!$ counts the number of ways to arrange n objects in a certain order. Each ordering can also be referred to as a **permutation**. For example, 1,3,2,4,5 is a permutation of the digits 1,2,3,4,5.

Exercise. Show that the number of ways to order any m objects from a set of n objects, where $m \leq n$, is $\frac{m!}{n!}$.

Now consider a similar, but different question:

> **Example 6.18.** The Math Club of Newton High School has 8 board members. They must elect a committee of 3 people to serve as directors. How many ways are there to do this? Note that there is no difference between the director positions.

Solution. At first glance, this may seem like a simple constructive counting problem that we have already done. There are 8 choices for the first director, 7 for the second, and 6 for the third– so our answer should be $8 \times 7 \times 6$.

However, we have overcounted; the 3 director positions are not distinct. For example, choosing Aspara, then Brussel, then Kale as our directors is the same choosing Kale, then Brussel, then Aspara, but we counted both in our previous calculation.

So, how many times have we overcounted? Suppose one of our possible committees is Aspara, Brussel, and Kale. There are $3! = 6$ ways to order the following 3 people, each of which were counted in our original calculation. In other words, we counted each possible committee *6* times. Thus, the number of possible committees is equal to

$$\frac{8 \times 7 \times 6}{3 \times 2 \times 1} = 56$$

■

Picking a few elements from a set of elements where the order in which they are chosen doesn't matter is a common theme in combinatorics problems. Note that if a problem uses words such as "committee" or "combination," it likely implies that order does not matter.

Example 6.19. Find a general formula for the number of ways to pick a committee of m people from a pool of n people.

Solution. First, we must pick m people in a constructive counting manner, for which there are

$$n \times (n-1) \cdots \times (n-m+1)$$

ways to do so. We can rewrite this as

$$\frac{n!}{(n-m)!}$$

Then, we must divide to compensate for overcounting. We counted each possible committee $m!$ times because we counted every possible permutation of each committee. Therefore, we must divide by $m!$. The number of ways to pick a committee of m people from a pool of n people is

$$\frac{n!}{(n-m)!m!}$$

■

This notation is slightly messy, so it is convention to use the following notation. For nonnegative integers n, m where $n \geq m$,

$$\binom{n}{m} = \frac{n!}{(n-m)!m!}$$

We call this combination notation because the each unique committee that can be put together is a **combination**. However, $\binom{n}{m}$ is also verbally referred to as "n choose m" because it is the number of ways you can choose m elements from a set of n elements with no regards to the order in which they are chosen.

Remark. When simplifyinh with fractions involving factorials, make sure to cancel out as many factors as possible between the numerator and denominator before multiplying anything.

Now let's look at an AMC problem involving combinations.

Example 6.20. (2017 AMC 10A) At a gathering of 30 people, there are 20 people who all know each other and 10 people who know no one. People who know each other hug, and people who do not know each other shake hands. How many handshakes occur within the group?

Solution. We can split the handshakes into two categories: those that occur between the 10 people that do not know anyone and those that occur between the group of 20 people and the group of 10 people. There are $\binom{10}{2} = 45$ handshakes in the first category because each possible combination of 2 people produces 1 handshake. There are $20 \times 10 = 200$ handshakes in the second category because there are 20 choices for one participant of the handshake and 10 for the other. Thus, there are $200 + 45 = 245$ handshakes in total. ■

Exercise. Solve this using complementary counting.

Example 6.21. We want to choose two disjoint committees of 4 people from a class of 12. How many ways can we do this, if the committees are distinct?

Solution. Note we can choose the first committee in $\binom{12}{4}$ ways and the second in $\binom{8}{4}$ ways (since the first 4 students are already in the first committee). Thus the answer is $\binom{12}{4} \cdot \binom{8}{4} = 34650$. ■

Now, we will move on to a slightly more complicated application of combinations.

Example 6.22 (2013 AIME I)**.** Melinda has three empty boxes and 12 textbooks, three of which are mathematics textbooks. One box will hold any three of her textbooks, one will hold any four of her textbooks, and one will hold any five of her textbooks. If Melinda packs her textbooks into these boxes in random order, the probability that all three mathematics textbooks end up in the same box can be written as $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

Solution. First, we will use constructive counting with combinations to find the total number of ways to distribute the 12 books. There are a total of $\binom{12}{3}$ ways to place a combination of three books in the first box and $\binom{9}{4}$ ways to place a combination of 4 books from the remaining 9 books into the second box. The 5 remaining books must be placed into the last box, so there is exactly 1 way to do so. Thus, there are a total of

$$\begin{aligned}\binom{12}{3} \cdot \binom{9}{4} \cdot 1 &= \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 1 \cdot 4 \cdot 3 \cdot 2 \cdot 1} \\ &= 11 \cdot 10 \cdot 9 \cdot 4 \cdot 7\end{aligned}$$

ways to place distribute the 12 books.

Now, we count the number of ways to distribute the books when all 3 math books are in the same box. We will do this with casework:

- Case 1: The 3 math books end up in the box with three books. There are $\binom{9}{4} = 126$ ways to distribute the remaining books.
- Case 2: The 3 math books end up in the box with four books. Now, we must pick one other book to be in the same box and then distribute the remaining books among the other two boxes. There are $\binom{9}{1}\binom{8}{3} = 504$ ways to do so.
- Case 3: The 3 math books end up in the box with five books. Now, we must pick two other books to be in the same box and then distribute the remaining books among the other two boxes. There are $\binom{9}{2}\binom{7}{3} = 1260$ ways to do so.

Adding them all up, there are a total of 1890 ways to distribute the books if all three math books are together. Thus, the probability that all three math books end up together is equivalent to

$$\frac{1890}{11 \cdot 10 \cdot 9 \cdot 4 \cdot 7} = \frac{3}{44}.$$

Therefore, $m + n = 3 + 44 = 47$. ■

Exercise.

(a) Compute $\binom{7}{3}$.
(b) Compute $\binom{7}{4}$.
(c) Compute $\binom{9}{2}$.
(d) Compute $\binom{9}{7}$.

Exercise. Show that $\binom{n}{m} = \binom{n}{n-m}$ is true, both in terms of counting objects and algebraically.

Now we'll move onto a rather hard example involving combinations that makes use of the idea of a one-to-one correspondence. We'll return to this idea in later handouts, as it will come in handy for proving a lot of things in combinatorics.

Example 6.23. For nonnegative integers a and b with $a + b \leq 6$, let $T(a, b) = \binom{6}{a}\binom{6}{b}\binom{6}{a+b}$. Let S denote the sum of all $T(a, b)$, where a and b are nonnegative integers with $a + b \leq 6$.

Solution. Directly summing the product of these binomial coefficients looks like it would be an algebraic mess. In problems involving obvious counting-related expressions like combinations, its often a good idea to think of a **counting argument**, or double counting. A counting argument is essentially a way of showing that two expressions count the same thing, which then means the two expressions are equal.

Let's look at each individual term $T(a, b)$ first. What could this possibly represent?

We can think of having 3 sets with 6 objects each. We pick a from the first set, b from the second set, then $a + b$ from the third set.

Here's the key observation: since

$$\binom{6}{a+b} = \binom{6}{6-a-b},$$

we can say we are choosing $6 - a - b$ objects from the third set instead of $a + b$ objects.

Then we are choosing a total of $(6 - a - b) + a + b = 6$ objects out of a set of 18 objects. In fact, we are choosing all such possible combinations of 6 objects out of 18 since $a + b$ can vary from 0 to 6.

This is just $\binom{18}{6}$. After some computation, this gives an answer of 18564. ■

Note how we showed both $\binom{18}{6}$ and the expression given in the problem counted the same abstract idea. Such arguments are the essence of combinatorics. Counting arguments won't appear very often on math competitions, but they are still very worthwhile to learn.

Exercise 6.24. Show that

$$\sum_{k=0}^{n} \binom{n}{k} = 2^k$$

using a counting argument. **Hint:** Think about sets and subsets.

§6.6 Homework Problems

Problem 6.1. [3] [2009 AMC 10B] How many 7-digit palindromes (numbers that read the same backward as forward) can be formed using the digits 2, 2, 3, 3, 5, 5, 5?

Problem 6.2. [4] [2004 AIME II] How many positive integers less than 10,000 have at most two different digits?

Problem 6.3. [5] [2012 AIME II] At a certain university, the division of mathematical sciences consists of the departments of mathematics, statistics, and computer science. There are two male and two female professors in each department. A committee of six professors is to contain three men and three women and must also contain two professors from each of the three departments. Find the number of possible committees that can be formed subject to these requirements.

Problem 6.4. [5] [2017 AMC 10A] Alice refuses to sit next to either Bob or Carla. Derek refuses to sit next to Eric. How many ways are there for the five of them to sit in a row of 5 chairs under these conditions?

Problem 6.5. [7] [2006 AIME II]

Let $(a_1, a_2, a_3, \ldots, a_{12})$ be a permutation of $(1, 2, 3, \ldots, 12)$ for which $a_1 > a_2 > a_3 > a_4 > a_5 > a_6$ and $a_6 < a_7 < a_8 < a_9 < a_{10} < a_{11} < a_{12}$. An example of such a permutation is $(6, 5, 4, 3, 2, 1, 7, 8, 9, 10, 11, 12)$. Find the number of such permutations.

Problem 6.6. [8] [2013 AMC 10A] Central High School is competing against Northern High School in a backgammon match. Each school has three players, and the contest rules require that each player play two games against each of the other school's players. The match takes place in six rounds, with three games played simultaneously in each round. In how many different ways can the match be scheduled?

Problem 6.7. [10] [2018 PUMaC] In an election between A and B, during the counting of the votes, neither candidate was more than 2 votes ahead, and the vote ended in a tie, 6 votes to 6 votes. Two votes for the same candidate are indistinguishable. In how many orders could the votes have been counted? One possibility is $AABBABBABABA$.

Problem 6.8. [7] [2016 AMC 10B]A set of teams held a round-robin tournament in which every team played every other team exactly once. Every team won 10 games and lost 10 games; there were no ties. How many sets of three teams $\{A, B, C\}$ were there in which A beat B, B beat C, and C beat A?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

7 More Counting Methods

In this handout, we'll go over a few specialized counting methods that appear often on the AMC and AIME.

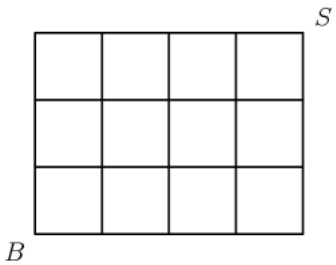
§7.1 Grid Paths

Let's say we have a person at point A on a 2-dimensional grid trying to reach another point B on the grid. However, the person can only move across adjacent points on the grid. How many different paths are there from A to B?

This idea of counting grid paths is very common. Now we'll dive into some examples to see how to solve these kinds of problems.

Example 7.1. Bob is stuck at home, which is located at the origin of an arbitrary Cartesian coordinate system. He wants to buy some food at the supermarket, which is 3 units up and 4 units left of his home (so at $(4, 3)$). Because he can only walk across sidewalks, Bob can only go in directions parallel to the axes. Also, because Bob doesn't want to waste time, he wants to travel exactly 7 units. How many ways can he walk to the supermarket?

First things first: draw a diagram.



Now, note that Bob can only go one unit at a time, and he can only go in the up and right direction since he can't travel more than 7 units.

There are several possibilities. He can go up 3 units and left 4 units, go left 4 units then up 3 units, or some path in between. Let's model a move up as U and a move right as R. Since Bob can move up exactly 3 times and he can move right exactly 4 times, his sequence of moves can be any permutation of $3U$'s and $4R$'s.

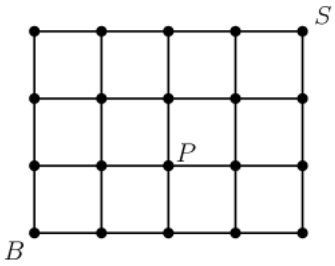
We've done this before! How many ways can you arrange 3 Us and 4 Rs? We can just choose which of the seven positions will contain a U, so our answer is

$$\binom{7}{3} = 35$$

Exercise. Show that the original problem and our new problem of arranging U's and R's are in a one-to-one correspondence.

There can also be restrictions that can make the problem trickier:

Example 7.2. Assume the same problem as last time, but there is a police station at $(2, 1)$ and Bob does not want to be at that point. How many paths can Bob take en route to the supermarket?



Solution. Since it's more straightforward to count paths crossing through the police station, we'll use complementary counting.

To do this, we need to find how many paths there are from B to P and multiply this by the number of paths from P to S; since every path we're looking for passes through the police station, it must be a composition of a path going to the police station and a path leading out.

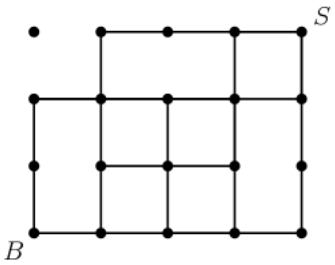
There are $3 \times 3 = 9$ paths that cut through the police station. (Verify the results yourself.) Thus, there are

$$35 - 9 = 26$$

ways to avoid the police department. ■

We can also have irregular grid patterns.

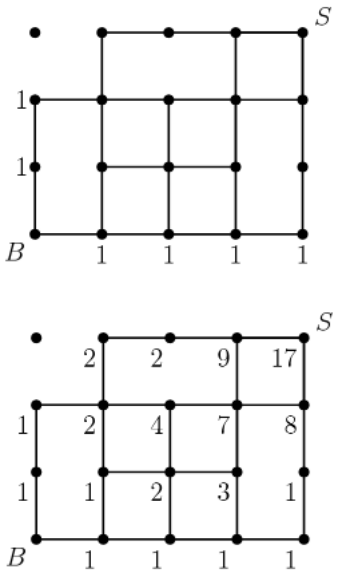
Example 7.3. Bob moves to another city, where the grid pattern is shown below. If he only goes up and right, how many paths does Bob have to get to the supermarket?



Solution. It appears that our current method cannot handle this complex system. When all else fails, we can use a recursive approach.

Label a number at every point that signifies how many paths lead up to that point. This number can be determined by adding the numerical values of the points immediately below and to the left of the point, since a point can be reached by taking any path to the point below then moving up, or by taking any path to the point to the left then moving right, and in no other way since the only possible moves are up or right.

We will illustrate how this works. First, we can fill in the edges with 1 since there's only one possible way to travel to any of the edge points: We can fill in the rest by adding the two



numbers that lead to it (the number to the left and the number below). Verify that the numbers we filled in are correct. The answer is 17.

■

Now, let us apply this to an actual competition problem.

Example 7.4 (1992 AIME). In a game of Chomp, two players alternately take bites from a 5-by-7 grid of unit squares. To take a bite, a player chooses one of the remaining squares, then removes ("eats") all squares in the quadrant defined by the left edge (extended upward) and the lower edge (extended rightward) of the chosen square. For example, the bite determined by the shaded square in the diagram would remove the shaded square and the four squares marked by $\times$. (The squares with two or more dotted edges have been removed form the original board in previous moves.)

The object of the game is to make one's opponent take the last bite. The diagram shows one of the many subsets of the set of 35 unit squares that can occur during the game of Chomp. How many different subsets are there in all? Include the full board and empty board in your count.

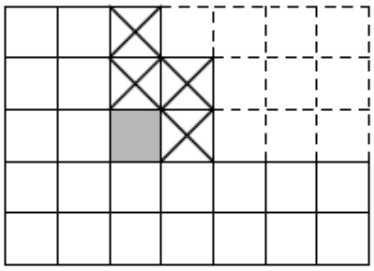
Solution. We strongly advise you to experiment with different subsets of the board first, and see if you can relate this problem to grid paths without reading further.

At first, it seems that there are no "paths" in this game. We'll have to find them ourself.

Instead of paths, we can think about lines of division. Note that the shaded square in each circumstance actually divides the grid into two parts: One with unchomped squares and one with chomped and to-be-chomped squares (the latter of which forms a rectangle).

We can configure a "path" by tracing the border of the unchomped squares. Specifically, we can do the following:

Assume that unit squares not shown (outside of the rectangle) are chomped already. Start at the upper left corner and only move along segments that are shared by both a chomped and an unchomped square (crossed and shaded squares are unchomped).



We will illustrate with the example above. If the lower left corner of the rectangle is the origin, and each square is a unit square, our path looks like this:

$$(0,5) \to (3,5) \to (3,4) \to (4,4) \to (4,2) \to (7,2) \to (7,0)$$

Convince yourself that finding the number of paths that only go right and down is in a one-to-one correspondence to the above problem. When you do, it should be clear that the answer is

$$\binom{7+5}{5} = 792$$

■

As with most hard counting problems, the most important step was realizing we could use a simple method that at first didn't seem to apply to the problem. You'll need to think of clever ways to apply the material in the handout to the homework problems similarly.

§7.2 Stars and Bars

Stars and Bars is a method of counting essential to problem solving.

We begin with a motivating example:

> **Example 7.5.** There are three dogs and you have ten identical toys. How many ways are there to distribute all of the toys to the dogs?

Solution. This seems like a hassle to count directly; we'd have to split by cases depending on how many toys go to each dog.

Instead, we can create a depiction of the ten toys as circles: How can we divvy up these toys?

We can start by using two dividers between the circles to distinguish between the three dogs. Each divider will be represented by a single line.

In the above example, we gave the first dog 2 toys, the second dog 0 toys and the third dog with 8 toys.

Amazingly, just by moving the dividers, we can count the number of ways to distribute the toys.

Exercise. Show that the original problem and the new problem of ordering dividers and circles are in a one to one correspondence.

We can find the answer as follows:

$$\binom{10+2}{2} = \binom{12}{2} = 66$$

■

We can apply this to algebraic equations too.

Example 7.6. How many solutions are there to the equation

$$a+b+c+d=14$$

where a, b, c, and d are non-negative integers?

Solution. We can think about this as taking 14 identical objects and distributing them to four boxes (i.e. our variables). This is the same situation as before. If we use 3 dividers to distinguish the 4 variables, we see that there are

$$\binom{14+3}{3} = \binom{17}{3} = 680$$

■

Let us solve a slightly different problem now:

Example 7.7. How many solutions are there to the equation

$$a+b+c+d=14$$

where a, b, c, and d are positive integers?

Solution. This time, all integers must be positive. This restriction is easy to take care of. Of the 14 objects, allocate one object to each of the four boxes automatically.

Now we've just reduced this problem to distributing $14-4=10$ objects to 4 boxes; it's just the case with nonnegative integers again, but with 10 instead of 14.

Thus, the answer is simply

$$\binom{10+3}{3} = \binom{13}{3} = 286$$

■

Now let's apply this to a hard problem:

Example 7.8 (2011 AIME II)**.** Ed has five identical green marbles, and a large supply of identical red marbles. He arranges the green marbles and some of the red ones in a row and finds that the number of marbles whose right hand neighbor is the same color as themselves is equal to the number of marbles whose right hand neighbor is the other color. An example of such an arrangement is GGRRRGGRG. Let m be the maximum number of

> red marbles for which such an arrangement is possible, and let N be the number of ways he can arrange the $m+5$ marbles to satisfy the requirement. Find N.

Solution. A simpler way to put the problem condition is that the number of color continuations (GG and RR) found in the row must be the same as the number of color switches (GR and RG). Because of this, if we wanted to add as many red marbles as we could, we would be limited by the number of color switches. Therefore, we want this limit of color switches to be rather high.

The maximum number of color switches is 10, found in the sequence

$$RGRGRGRGRGR.$$

We have 0 color continuations here. Now, we should add more red marbles to the end to increase the amount of these continuations. We end up with 16 red marbles.

Now we have to order these to keep the equality of continuations and switches. We can place these red marbles anywhere but since they are indistinguishable, we have to use stars and bars to count them. Note that we have 10 stars, which are the unused red marbles we wish to place, and 5 bars, which are the green marbles. This gives us an answer of

$$\binom{10+5}{5} = 3003.$$

■

Exercise 7.9. How many solutions are there to the equation

$$a+b+c+d \leq 14$$

where a, b, c, and d are non-negative integers? (Note: Be creative! When you figure out the solution, the computation is almost exactly the same as in Example 7.6.)

§7.3 Symmetry

From previous counting problems, you've already seen the possibility of *overcounting*, or counting the same object multiple times. Sometimes two objects can be the "same", or symmetric, if they have been transformed in some way that preserves their shape. The most common types of symmetry are reflectional symmetry and rotational symmetry.

Definition 7.10. A **reflection** is a mirrored image across a line (in two dimensions). In three dimensions, reflections are mirrored images across planes. Two objects have **reflectional symmetry** if they are reflections of each other.

For example, an isosceles triangle has reflectional symmetry, where the line of symmetry is the altitude to the side of different length.

Definition 7.11. An object has **rotational symmetry** if it can be rotated through by an angle $0 \leq \theta < 2\pi$ and remain the same. We say an object has n-fold symmetry iff there are n distinct angles $0 \leq \theta < 2\pi$ that it can be rotated and stay the same.

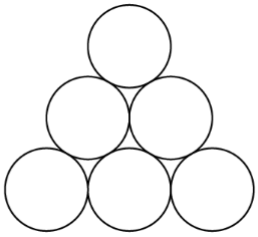
Consider a square; it clearly has 4-fold symmetry, as we can rotate by $0, \pi/2$, π or $3\pi/2$ and end up with the same image. Similarly, any regular n-gon will have n-fold symmetry. It is visually intuitive that a regular n-gon has d-fold symmetry iff d is a positive divisor of n. For example, an octagon also has 4-fold and 2-fold symmetry.

Exercise. Prove that *any* object with n-fold symmetry also has d-fold symmetry whenever d is a positive divisor of n.

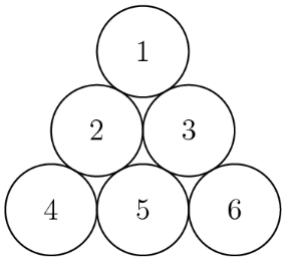
From now on, whenever we refer to n-fold symmetry, n is maximal: so, for example, we will only refer to a square as having 4-fold symmetry.

In counting problems with reflections and rotations, the strategy is often to use casework so we avoid overcounting certain configurations.

Example 7.12 (2017 AMC 10B)**.** In the figure below, 3 of the 6 disks are to be painted blue, 2 are to be painted red, and 1 is to be painted green. Two paintings that can be obtained from one another by a rotation or a reflection of the entire figure are considered the same. How many different paintings are possible?



Solution. Let's label the disks as follows:



There aren't that many possible cases because reflections and rotations are equivalent, so we can choose a location for the three blue disks and then figure out the number of paintings for each location. After playing around for a while, it's easy to see there are 6 distinct locations for the blue disks with respect to reflection and rotation. We'll do cases based on each set of locations.

Case 1 $(1, 2, 3)$

All that remains is the bottom row; we can either place the green disk in the middle or on either edge of the bottom row (placing it on either edge is equivalent by reflection). So we have 2 paintings.

Case 2 $(1, 2, 4)$

We can put the green disk in the 6 spot and the red disks in 3 and 5. We can also put the green disk in 3 or 5; both are the same by reflection, so we get 2 more paintings.

Case 3 $(1, 2, 5)$

Here every position of the green disk is distinct so we have 3 paintings in this case.

Case 4 $(1, 2, 6)$

Again, each position of the green disk is unique, so we have 3 paintings again.

Case 5 $(1, 4, 6)$

This leaves the center 3 disks. Putting the green disk in any of the three remaining spots and the red disks in the remaining spots is equivalent by rotation, so we have 1 distinct painting.

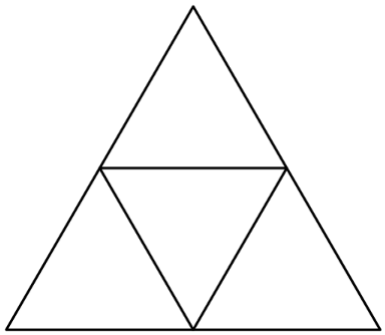
Case 6 $(2, 3, 5)$

Any placement of the green disk and red disks is the same by rotation so there is 1 painting.

Adding up the 6 cases gives us a total of $2 + 2 + 3 + 3 + 1 + 1 = 12$ paintings. ■

Example 7.13 (2006 AIME). There is an unlimited supply of congruent equilateral triangles made of colored paper. Each triangle is a solid color with the same color on both sides of the paper. A large equilateral triangle is constructed from four of these paper triangles. Two large triangles are considered distinguishable if it is not possible to place one on the other, using translations, rotations, and/or reflections, so that their corresponding small triangles are of the same color.

Given that there are six different colors of triangles from which to choose, how many distinguishable large equilateral triangles may be formed?



Solution. Label the top triangle "1", the bottom-right triangle "2" and the bottom-left triangle "3". Let's see what we can do using reflections and rotations.

We see that by using rotation, we can make the top triangle either "1", "2", or "3". Then the two bottom numbers can be switched by reflecting across the line of symmetry from the top vertex to the base. Reflections and rotations cannot change the position of the center triangle.

Thus, assuming the center triangle's color is fixed, only the combination of colors we use for the outer triangles matters, not their order. That is, any two triangles with the same center triangle color, and the same multiset(i.e. set including repeats) of colors for the outside triangles are the same. So we can split this into cases based on how many distinct colors there are for the outer triangles.

Case 1 (3 distinct colors) There are $\binom{6}{3}$ choices for the outer colors since we have 6 colors to choose from and order does not matter. The center triangle can be any of the 6 colors, so we get $6\binom{6}{3} = 120$.

Case 2 (2 distinct colors) If there are 2 distinct colors then one color appears twice and the other appears once. There are 6 possibilities for the color that appears twice and $6 - 1 = 5$ for the color that appears once since the two colors must be distinct. Finally, the center triangle can be any of the 6 colors, giving us $6 \cdot 6 \cdot 5 = 180$ triangles for this case.

Case 3 (1 color) We choose one color for all the outside triangles and one for the center triangle, yielding $6 \cdot 6 = 36$.

Adding up the cases, we get an answer of

$$120 + 180 + 36 = 336.$$

■

Example 7.14. How many ways can we color the vertices of a regular octagon either red, blue, or green, where colorings are considered the same if they are rotations of each other?

Solution. Let's start by considering the total amount of colorings without the rotation condition, which is 3^8. What are we overcounting?

For a coloring with no symmetry, we know we overcount it by a factor of 8 as each of its 8 rotations is counted. However, colorings with symmetry are different; if a coloring has n-fold symmetry, then we only count it $8/n$ times (since its coloring pattern repeats $8/n$ times if we rotate it 8 times by an angle of $\pi/4$).

We know that the coloring can have 8-fold, 4-fold, or 2-fold symmetry, or no symmetry. Let's consider each of these cases independently, initially considering rotations distinct.

Case 1 (8-fold symmetry)

If we have 8-fold symmetry, then every vertex must be colored the same, so there are 3 colorings in this case.

Case 2 (4-fold symmetry)

An octagon with 4-fold symmetry is determined by the coloring of any two adjacent vertices (the 2-vertex coloring simply repeats 3 more times), so we have a count of $3^2 = 9$. But by doing this we also counted the colorings with 8-fold symmetry, so we have to subtract them out to get a total of $9 - 3 = 6$ in this case.

Case 3 (2-fold symmetry)

Here we need a coloring of $8/2 = 4$ adjacent vertices that will be used twice. We can color 4 vertices in $3^4 = 81$ ways, but we need to subtract the colorings with 4-fold and 8-fold symmetry, so we have a total of $81 - 6 - 3 = 72$.

Case 4 (no symmetry)

The total possible number of colorings is 3^8, and subtracting out colorings with symmetry, we get $3^8 - 72 - 6 - 3 = 6480$. Now for each case with n-fold symmetry, we overcounted by a factor of $8/n$, so we have a final answer of

$$\frac{3}{1} + \frac{6}{2} + \frac{72}{4} + \frac{6480}{8} = 834.$$

■

Exercise. Try solving this problem where the octagon is replaced with a regular 9-gon.

Symmetry will come up often in counting problems that have some kind of visual or geometrical context, so you should always consider symmetry when avoiding overcounting. Symmetry can also be useful in speeding up casework; if some cases are symmetric, you can group them together to save time.

§7.4 Homework Problems

Problem 7.1 (2018 AMC 10A)**.** [5]When 7 fair standard 6-sided dice are thrown, the probability that the sum of the numbers on the top faces is 10 can be written as

$$\frac{n}{6^7},$$

where n is a positive integer. What is n?

Problem 7.2 (2019 AMC 8)**.** [5] Alice has 24 apples. In how many ways can she share them with Becky and Chris so that each of the three people has at least two apples?

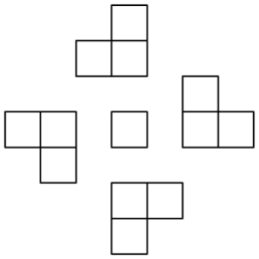
Problem 7.3 (2010 AMC 12A)**.** [7]A 16-step path is to go from $(-4, -4)$ to $(4, 4)$ with each step increasing either the x-coordinate or the y-coordinate by 1. How many such paths stay outside or on the boundary of the square $-2 \le x \le 2$, $-2 \le y \le 2$ at each step?

Problem 7.4 (2014 AMC 10B)**.** [7] The numbers $1, 2, 3, 4, 5$ are to be arranged in a circle. An arrangement is *bad* if it is not true that for every n from 1 to 15 one can find a subset of the numbers that appear consecutively on the circle that sum to n. Arrangements that differ only by a rotation or a reflection are considered the same. How many different bad arrangements are there?

Problem 7.5 (2018 AMC 12A)**.** [8] A scanning code consists of a 7×7 grid of squares, with some of its squares colored black and the rest colored white. There must be at least one square of each color in this grid of 49 squares. A scanning code is called *symmetric* if its look does not change when the entire square is rotated by a multiple of 90° counterclockwise around its center, nor when it is reflected across a line joining opposite corners or a line joining midpoints of opposite sides. What is the total number of possible symmetric scanning codes?

Problem 7.6 (2012 AMC 10A)**.** [8] A 3×3 square is partitioned into 9 unit squares. Each unit square is painted either white or black with each color being equally likely, chosen independently and at random. The square is then rotated 90° clockwise about its center, and every white square in a position formerly occupied by a black square is painted black. The colors of all other squares are left unchanged. The probability the grid is now entirely black can be represented as $\frac{p}{q}$, where p and q are relatively prime positive integers. What is $p + q$?

Problem 7.7 (2013 AIME I)**.** [7] In the array of 13 squares shown below, 8 squares are colored red, and the remaining 5 squares are colored blue. If one of all possible such colorings is chosen at random, the probability that the chosen colored array appears the same when rotated 90 degrees around the central square is $\frac{1}{n}$, where n is a positive integer. Find n.



Problem 7.8 (2007 AIME I)**.** [10] In a 6 x 4 grid (6 rows, 4 columns), 12 of the 24 squares are to be shaded so that there are two shaded squares in each row and three shaded squares in each column. Let N be the number of shadings with this property. Find the remainder when N is divided by 1000.

Problem 7.9 (2003 AMC 12A)**.** [7] Objects A and B move simultaneously in the coordinate plane via a sequence of steps, each of length one. Object A starts at $(0, 0)$ and each of its steps is either right or up, both equally likely. Object B starts at $(5, 7)$ and each of its steps is either to the left or down, both equally likely. The probability that the objects meet can be represented as $m/2^n$ for positive integers m and n where m is not divisible by 2. What is $m + n$?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

8 PIE, States & Recursion

§8.1 Recursion

In this section, we'll go over recursion. Recursion is a common tool on the AIME that should be considered for any hard counting problem. This concept is very challenging, so you should take extra effort to try and understand each step in our example problems.

We'll start with a motivating example.

> **Example 8.1** (Classical). Suppose that we have a ten-step staircase. Liam starts at the bottom, and every second, he may either climb one step or climb two steps. How many ways can he ascend the staircase? (One way might be to climb two steps, then one step, then two steps, then one steps five more times.)

Solution. This problem seems annoying to do with standard methods—we might be able to do casework on the number of two-step climbs Liam attempts, but this is really computational.

To begin solving most math problems, it helps to consider small cases. If we deal with a one-step staircase, there's only one way for Liam to climb it. For a two-step staircase, Liam can either climb one step twice or climb two steps, which makes for two ways. In a similar manner, we can count the first few cases:

Height of Staircase	Ways to Climb
1	1
2	2
3	3
4	5
5	8

(You should confirm for yourself that these numbers are correct!)

At this point, a pattern begins to emerge: the number of ways to climb the staircase appears to follow the Fibonacci Sequence.

To see why this might be the case, we think about how the Fibonacci sequence works in the first place: each successive term of the sequence is built on the previous two terms. Suppose that Liam currently stands on the nth step of the staircase. He must have gotten there from the $(n-1)$th step or the $(n-2)$th step, because he can only climb one or two steps at a time.

Therefore, the number of ways for Liam to climb to step n is equal to the number of ways he can climb to step $n-2$ and then climb two steps, added to the number of ways he can climb to step $n-1$ and then climb one step. (If you're right now asking why he can't climb to $n-2$ and take a single step to $n-1$, this case is addressed in the $n-1$-case already!) Expressed mathematically, if S_i denotes the way for Liam to climb an i-step staircase, we have

$$S_n = S_{n-1} + S_{n-2}.$$

Thus the number of distinct ways to ascend n steps is equal to the number of ways to ascend $n-1$ steps added to the number of ways to ascend $n-2$ steps — which is exactly the Fibonacci

sequence, expressed differently. Now the remaining computation is easy: finishing the table yields that if the staircase has 10 steps, then there are 89 distinct ways to ascend it. ■

It would have been really difficult to do pure casework on the number of two-step ascensions, or some other method! The idea of recursion here is that the process of climbing some number n of steps — in this case, 10 — is linked to the process of climbing $n-1$ steps or $n-2$ steps. You should try another classical exercise before moving on.

Exercise 8.2 (Classical). How many ways are there to fill in a 2×10 grid with 1×2 dominos?
Hints: Relate 2×10 to $2 \times n$ for some smaller n than 10 by thinking about horizontal or vertical placement at the end!

Recursion, simply put, is the process of using smaller cases of a problem to build up to a solution for larger cases. Recursion in combinatorics is similar to having a recursive sequence (e.g. we found the Fibonacci sequence in the previous example), except the "sequence" is a function $f(n)$ that counts the nth case of a problem; for example, $f(n)$ often counts the number of strings of length n satisfying certain conditions, but it could also count the number of ways a traveling object can reach a certain location in n steps and a variety of other things.

To solve a problem using recursion, we have to find $f(n)$ in terms of solely $f(n-1), f(n-2), \ldots f(1)$. Then we can make a table of values and compute values of $f(n)$ recursively. Recursion has many parallels with induction in that we have base cases and we use some kind of relation to go from the base cases to case n, except we often do actual computation rather than finding some general formula.

Recursion can also be used in the context of probability, where our recursive function might be defined as the probability an object has a certain state after n moves, or the probability it will reach a point P. This often happens with problems involving a moving object with certain limitations.

Recursion is best illustrated by example. Let's look at some competition problems.

Example 8.3 (2019 OMO). Susan is presented with six boxes $B_1, \ldots, B_6$, each of which is initially empty, and two identical coins of denomination 2^k for each $k = 0, \ldots, 5$. Compute the number of ways for Susan to place the coins in the boxes such that each box B_k contains coins of total value 2^k.

Solution. Say the number of ways to solve the problem for n boxes is $F(n)$. We instead solve the problem for general n (motivated by trying small cases).

We look at the number of ways we can distribute the coins of value 2^{n-1}. We can either put both of them in B_n or one of them in B_n and the other in B_{n-1}. Notice these are the only two possibilities since 2^{n-1} is too big to go anywhere else.

Now notice that in the first case, it remains to fill boxes with capacities $2^1, 2^2, \ldots, 2^{n-1}$ with two coins each of values $2^0, 2^1, \ldots, 2^{n-2}$. In the second case, it's actually the same, since we need 2^{n-1} more to fill box B_n so it is effectively a box with capacity 2^{n-1}.

Thus, we've reduced the n case to the $n-1$ case. Since there are two ways to distribute the coins of value 2^{n-1}, $F(n) = 2F(n-1)$.

Obviously $F(1) = 1$. So $F(n) = 2^{n-1}$ and $F(6) = 32$. ■

Example 8.4. (2008 AIME I) Consider sequences that consist entirely of A's and B's and that have the property that every run of consecutive A's has even length, and every run of consecutive B's has odd length. Examples of such sequences are AA, B, and $AABAA$, while $BBAB$ is not such a sequence. How many such sequences have length 14?

Solution. There are many hints in this problem to use recursion. First of all, it's a problem about strings of As and Bs, but the consecutive condition also suggests recursion as what we can append to a string depends on the previous characters in the string.

So let's say we have a string of length n satisfying the given conditions. Can we break it down into a smaller string?

It depends on what the last character of the string is. If the string ends in an A, then we know that the last two characters are AA since there must be an even number. Then removing the last two characters should still leave us with a string satisfying the conditions.

This means that every string of length n ending in A is just another string of length $n-2$ satisfying the conditions with an AA appended at the end. If the string ends in a B then it must end in an odd number of Bs. If it only ends in one B, then removing the last character should give us a string ending in A satisfying the conditions. But if it ends in more than one B, we have to remove the last 2 characters to ensure the number of consecutive Bs is still odd.

Thus, every string of length n ending in B is either a string of length $n-1$ ending in A with a B appended at the end or a string of length $n-2$ ending in B with a BB appended at the end.

From these observations, it makes the most sense to define the recursive functions $a(n)$ and $b(n)$ as the number of sequences ending in A of length n and the number of sequence ending in B of length n, respectively. Then from our earlier statements, we have that

$$a(n) = a(n-2) + b(n-2)$$
$$b(n) = a(n-1) + b(n-2)$$

Then if we have the values of $a(1), a(2), b(1)$ and $b(2)$ we should be able to compute up to $a(14)$ and $b(14)$ recursively. From the problem statement it is easy to see that $a(1) = 0$, $a(2) = 1$, $b(1) = 0$, and $b(2) = 1$. Now we compute the rest of the values in a table:

n	$a(n)$	$b(n)$	n	$a(n)$	$b(n)$
1	0	1	8	6	10
2	1	0	9	11	11
3	1	2	10	16	21
4	1	1	11	22	27
5	3	3	12	37	43
6	2	4	13	49	64
7	6	5	14	80	92

So the answer is $a(14) + b(14) = 80 + 92 = \boxed{172}$. ■

A recursive approach can also be used in the coordinate plane, similar to what we saw in grid paths yesterday. Here is a fairly standard recursion problem involving probability:

Example 8.5. (2019 AIME I) A moving particle starts at the point $(4,4)$ and moves until it hits one of the coordinate axes for the first time. When the particle is at the point (a,b), it moves at random to one of the points $(a-1,b)$, $(a,b-1)$, or $(a-1,b-1)$, each with probability $\frac{1}{3}$, independently of its previous moves. The probability that it will hit the coordinate axes at $(0,0)$ is $\frac{m}{3^n}$, where m and n are positive integers. Find $m+n$.

Solution. Recursion seems like a promising tool to solve this problem; the particle can only move left and down, and the problem tells us where the particle can move based on where it previously was.

Then if we define $P(x,y)$ to be the probability the particle reaches point $(0,0)$ first if it starts at (x,y) we have that

$$P(x,y) = \frac{1}{3}P(x,y-1) + \frac{1}{3}(x-1,y) + \frac{1}{3}(x-1,y-1)$$

as there is a $\frac{1}{3}$ probability of going one unit up, one unit right, or one unit up and right.

We can make a 2-dimensional grid and recursively compute values (similar to how we counted grid paths in the previous handout) to get

$$P(4,4) = \frac{245}{2187} = \frac{245}{3^7},$$

giving us an answer of $245+7=\boxed{252}$. ■

§8.2 States

States are often used in conjunction with recursions. Essentially, we can use states to represent locations or situations of an object or character; then the object can move to another state. Let's take the basic example: a number line.

Overall, states involve a character moving around a plane, number line, or similar bijection with probabilities to move to different 'states'. Oftentimes, this is portrayed as a game of some sorts in the problem statement. Then, we can use a 'state' to represent where our character is, either on the number line or their progress in the game, and by doing so we can form equations out of our states. We first start with a very simple example.

Example 8.6 (2017 AMC 10A). Amelia has a coin that lands heads with probability $\frac{1}{3}$, and Blaine has a coin that lands on heads with probability $\frac{2}{5}$. Amelia and Blaine alternately toss their coins until someone gets a head; the first one to get a head wins. All coin tosses are independent. Amelia goes first. Find the probability that Amelia wins.

Solution. In this problem, since Amelia goes first, suppose the probability Amelia win's given that she's tossed k times is p_k. We know Amelia has a $1/3$ chance to win, but there is also a $2/3$ chance she'll fail to get a heads, so we proceed to the p_1 state. Thus,

$$p_0 = \frac{1}{3} + \frac{2}{3}p_1$$

Now, we note that at p_1, the only way for Amelia to win is if we can proceed to p_2. This happens at a $3/5$ chance, so we have that

$$p_1 = \frac{3}{5}p_2.$$

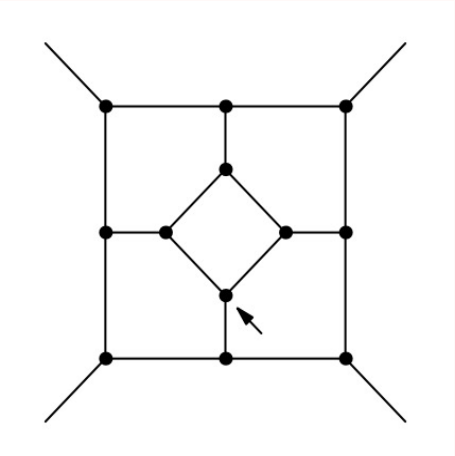
However, we realize that p_2 is exactly the same situation as p_0 because it is once again Amelia's turn. Hence, going back to our original equation, we have that

$$\begin{aligned} p_0 &= \frac{1}{3} + \frac{2}{3} \cdot \frac{3}{5} p_0 \\ p_0 &= \frac{1}{3} + \frac{2}{5} p_0 \\ p_0 &= \frac{5}{9} \end{aligned}$$

so the probability that Amelia wins is precisely $\frac{5}{9}$. While this problem doesn't fully exemplify the utility of states, it is a nice introductory problem to serve the concepts. ■

Now, let's take a look at a problem with more states.

Example 8.7. (2020 FAIME) Naveen is lost in the maze shown below, where rooms are labeled with dots, and paths between rooms are labeled with line segments. He is currently in the room indicated by the arrow. As long as he remains in the maze, Naveen repeatedly "moves" by randomly choosing one of the paths leading from the room where he is currently located to the next room. All choices are equally likely and independent of any moves he has previously made. He stops after he makes a move that leads him out of one of the maze's four exits. Compute the expected number of moves Naveen will make before he leaves the maze.



Solution. At first glance, it seems that states would be clearly be a bad idea. We're given a starting point but Naveen could really move anywhere, so are we supposed to use 12 states?

The real trick to this program is utilizing the symmetry to its full extent. As noted before, we would just have a mess of equations with 12 states. Suppose we break the diagram into 3 groups - the four corners of the large square, the four corners of the middle square, and the four midpoints of each side. Then, we create 3 states total, one for each group, and this cuts the amount of equations needed significantly. Before we actually create our states, we need to know what they are going to represent.

As opposed to the last problem, we want the expected number of moves instead of a probability. As such, we can make our lives a bit easier by getting rid of the n-th state, and simply instead let a be the expected number of moves from a center square point, b be the expected number of moves from a side midpoint, and c be the expected number of moves from a corner point. Naveen starts at a, so we'll try to solve for a. In order to do so, we must first set up our equations.

First, we'll try to construct the relations between a, b, c. From a, we can only move to 2 other a points or to a b point. Hence, we can set up the following equation:

$$a = 1 + \frac{2}{3}a + \frac{1}{3}b.$$

We add a one since we've made another move and must add it to our count. Similarly, we can construct the following equations:

$$b = 1 + \frac{2}{3}c + \frac{1}{3}a$$
$$c = 1 + \frac{2}{3}b + \frac{1}{3}0$$

We let 0 represent the end of the maze, since there are 0 moves left to make once we've left the maze.

Now, we can solve this system of equations without worry. Doing so gives $a = \boxed{15}$, so Naveen should get out of the maze in 15 moves. ■

When working with states, just remember that they are simply another method of recursion with a more visual component to them.

§8.3 PIE

In combinatorics, we very often have simple brute-force solutions to hard problems that would work, if not for overcounting. Usually we will have to yield and find another solution, perhaps proceeding to do tedious casework. However, the **Principle of Inclusion-Exclusion** gives us a systematic way of handling overcounting for certain kinds of problems, allowing us to quickly solve deceptively hard problems.

First, let's review some set notation. Recall that a **set** is an unordered collection of objects (usually numbers) with no repeats.

Definition 8.8. The **intersection** of two sets A and B, denoted $A \cap B$, is the set of elements they have in common.

Definition 8.9. The **union** of two sets A and B, denoted $A \cup B$, is the set of all elements in A and B.

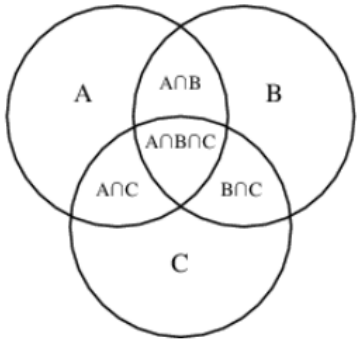
Definition 8.10. The **cardinality** of A, denoted $|A|$, is the number of elements in A.

Let's say we have two sets, A and B, and we want to find the cardinality of $A \cup B$. This should be the number of elements in A, plus the number of elements of B, minus their intersection. So we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Now what if we had three sets, A, B, and C? What would the cardinality of $A \cup B \cup C$ be? Let's draw a Venn diagram to make this clearer.

We can start with considering $|A| + |B| + |C|$. What do we need to subtract from this? If we look at the intersections on the Venn diagrams, we see that the elements in $A \cap B$, $A \cap C$, and $B \cap C$ have all been counted twice in this sum since each of these subsets lies in two of A, B, and C. So we need to subtract out $|A \cap B| + |A \cap C| + |B \cap C|$ to make sure we only count it



once. Now we have $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$. But we haven't considered $A \cap B \cap C$ yet; since these elements lie in all of $A, B, C, A \cap B$, $A \cap C$, and $B \cap C$, we count it three times, then subtract it out three times, meaning our current sum counts it zero times. So we need to add in $|A \cap B \cap C|$ to get our final answer of

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

In fact, this pattern continues for more than three sets; if we have n sets $A_1, A_2, \ldots A_n$, to find the cardinality of the union of all the sets, we add the cardinalities of all the sets, then subtract the cardinalities of pairwise intersections, then add the cardinalities of the intersections of all triplets of sets, then subtract the cardinalities of the intersections of all quadruplets of sets, and so on (see if you can prove this using the same intuition as in our Venn diagram of three sets). This result is known as the Principle of Inclusion-Exclusion.

Theorem 8.11 (Principle of Inclusion-Exclusion). *If we have n sets $A_1, A_2, \ldots A_n$, then the cardinality of $A_1 \cup A_2 \cup \cdots \cup A_n$ is*

$$\sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

If this is confusing to you, just remember that the sum contains the cardinality of the intersections of every possible combination of any number of the n sets, and the sign of each term is -1 to the power of the number of sets in the intersection.

We'll start with a very simple application.

Example 8.12 (Brilliant). At a construction site, Jorge is in charge of hiring skilled workers for the project. Out of 80 candidates that he interviewed, he found that

- 45 were painters,
- 50 were electricians,
- 50 were plumbers,
- 15 had skills in all three areas, and
- all of them had skills in at least one of these areas.

If he hired everyone who was skilled in exactly 2 areas, how many candidates were hired?

Let A denote set of painters, B denote the electricians, and C denote the plumbers. Then we want to find $|A \cap B| + |A \cap C| + |B \cap C|$. Let this sum be x. We know this sum is one of the terms in PIE, so we can apply that here. We know that

$$|A| + |B| + |C| - x + |A \cap B \cap C| = 80.$$

We are given the values of $|A|$, $|B|$, and $|C|$, and of $|A \cap B \cap C|$. Plugging them in gives

$$45 + 50 + 50 - x + 15 = 80$$

which means that $x = 80$.

Example 8.13 (2005 AMC 12A)**.** Call a number prime-looking if it is composite but not divisible by $2, 3$, or 5. The three smallest prime-looking numbers are $49, 77$, and 91. There are 168 prime numbers less than 1000. How many prime-looking numbers are there less than 1000?

Solution. The first thing we want to do is categorize exactly which numbers are prime-looking. Unfortunately, we don't know much about prime-looking numbers, but we know what they are *not*; numbers that are not prime-looking consist of those that are divisible $2, 3$, or 5 or are prime. So we'll use complementary counting to find the amount of numbers less than 1000 that are not prime-looking, then subtract that from 999.

First of all, we're given that there are 168 prime numbers less than 1000. We also know that 1 is neither prime nor composite. Then the only remaining not prime-looking numbers are numbers divisible by $2, 3$, or 5. We'll try counting this. (Note we have to subtract 3 afterwards since $2, 3$, and 5 are primes as well). If we let

$$\begin{aligned} S_2 &= \{\text{numbers less than 1000 divisible by 2}\} \\ S_3 &= \{\text{numbers less than 1000 divisible by 3}\} \\ S_5 &= \{\text{numbers less than 1000 divisible by 5}\} \end{aligned}$$

then we want to find $|S_2 \cup S_3 \cup S_5|$. We can use PIE to do this. By PIE,

$$|S_2 \cup S_3 \cup S_5| = |S_2| + |S_3| + |S_5| - |S_2 \cap S_3| - |S_3 \cap S_5| - |S_2 \cap S_5| + |S_2 \cap S_3 \cap S_5|.$$

It is quite easy to compute the cardinality of any of these intersections; for example, $|S_2 \cap S_3|$, is simply the number of positive integers less than 1000 divisible by $2 \times 3 = 6$, and $|S_2 \cap S_3 \cap S_5|$ is simply the number of positive integers less than 1000 divisible by $2 \times 3 \times 5 = 30$. We leave this computation to the reader, but we should get that

$$|S_2 \cup S_3 \cup S_5| = 499 + 333 + 199 - 166 - 66 - 99 + 33 = 733.$$

Subtracting out 3 gives us that there are 730 more not prime-looking numbers that are neither 1 nor prime. So the total number of not prime-looking numbers is $730 + 168 + 1 = 899$, giving us an answer of $999 - 899 = 100$. ■

That was a pretty standard application of PIE; in fact, you might have done something similar previously when counting multiples, without even knowing you were using PIE. Make sure you can rationalize why our use of PIE worked in that problem.

Now let's move on to a very challenging example that teaches us the importance of being organized with our sets.

Example 8.14. (Classical) A derangement is a permutation with no fixed points. That is, a derangement of a set leaves no element in its original place. For example, the derangements

of $(1, 2, 3)$ are $(2, 3, 1)$ and $(3, 1, 2)$, but $(3, 2, 1)$ is not a derangement of $\{1, 2, 3\}$ because 2 is a fixed point. Let D_n the number of derangements of $(1, 2, \dots n)$. Find D_n.

Solution. Since there's no easy way to count derangements, we can instead use complementary counting, and count the number of permutations that have at least one fixed point.

An obvious approach would be to choose one of the n points to fix, then permute the rest of the $n-1$ elements. This gives $n \times (n-1)! = n!$ permutations. But we are obviously overcounting here; for example, if a permutation fixes (i.e. does not move) 1 and fixes n, then we've counted it twice.

We can use PIE to deal with this overcounting. We have our n sets $A_1 \dots A_n$ where A_j consists of all permutations fixing j. Then $A_1 \cup A_2 \cdots \cup A_n$ will gives all permutations that fix at least one point, which is what we want.

Assume we have a k-tuple of these sets, $A_{i_1} \dots A_{i_k}$, where $i_1, i_2, \dots i_k$ are distinct integers between 1 and n inclusive. How many elements are in their union?

Well, the union of k such sets would simply be the number of permutations that fix the k elements $i_1 \dots i_k$. Since we are fixing k elements, and permuting the rest, there are $(n-k)!$ elements in each intersection of k sets. Furthermore, there are $\binom{n}{k}$ different combinations of k sets. So by PIE, we have that the number of permutations with atleast one fixed point is

$$\binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \cdots + (-1)^{n+1}\binom{n}{n}0!.$$

Since the total number of permutations is $n!$, our answer is

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^{n}\binom{n}{n}0!.$$

Since $\binom{n}{k}(n-k)! = \frac{n!}{k!}$, we can put this more concisely in summation notation as

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

■

Remark. Those of you who are familiar with calculus might notice that our answer is simply $n!$ times the the partial sum of the first n terms of the Maclaurin series expansion of $\frac{1}{e}$. Indeed, it turns out that

$$D_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor.$$

and that

$$\lim_{n\to\infty} \frac{D_n}{n!} = \frac{1}{e}.$$

In this problem, we used PIE on a variable number of sets; usually competition problems will be more concrete, and we'll have a known number of sets to work with. However, this problem gave us valuable insight; we started by considering a crude approach that obviously overcounted, then figured out how to use PIE to deal with that overcounting.

§8.4 Homework Problems

Problem 8.1. [3] [2017 AMC 10B] There are 20 students participating in an after-school program offering classes in yoga, bridge, and painting. Each student must take at least one of these three classes, but may take two or all three. There are 10 students taking yoga, 13 taking bridge, and 9 taking painting. There are 9 students taking at least two classes. How many students are taking all three classes?

Problem 8.2. [4] [2019 AMC 10A] How many positive integer divisors of 201^9 are perfect squares or perfect cubes (or both)?

Problem 8.3. [6] [2018 HMMT] Lil Wayne, the rain god, determines the weather. If Lil Wayne makes it rain on any given day, the probability that he makes it rain the next day is 75%. If Lil Wayne doesn't make it rain on one day, the probability that he makes it rain the next day is 25%. He decides not to make it rain today. Find the smallest positive integer n such that the probability that Lil Wayne makes it rain n days from today is greater than 49.9%.

Problem 8.4. [7] [2003 AIME II] A bug starts at a vertex of an equilateral triangle. On each move, it randomly selects one of the two vertices where it is not currently located, and crawls along a side of the triangle to that vertex. Find the probability that the bug moves to its starting vertex on its tenth move.

Problem 8.5. [8] [2019 AMC 10B] How many sequences of 0s and 1s of length 19 are there that begin with a 0, end with a 0, contain no two consecutive 0s, and contain no three consecutive 1s?

Problem 8.6. [9] [2016 PUMaC] The George Washington Bridge is 2016 meters long. Sally is standing on the George Washington Bridge, 1010 meters from its left end. Each step, she either moves 1 meter to the left or 1 meter to the right, each with probability $\frac{1}{2}$. What is the expected number of steps she will take to reach an end of the bridge? **Hint:** Consider symmetry about the point 1008 meters away from either end.

Problem 8.7. [10] [2019 AIME II]

While watching a show, Ayako, Billy, Carlos, Dahlia, Ehuang, and Frank sat in that order in a row of six chairs. During the break, they went to the kitchen for a snack. When they came back, they sat on those six chairs in such a way that if two of them sat next to each other before the break, then they did not sit next to each other after the break. Find the number of possible seating orders they could have chosen after the break. **Hint:** Consider using PIE where each of our sets contains all configurations where a certain pair is seated together.

Problem 8.8. [8] [2001 AIME I] A mail carrier delivers mail to the nineteen houses on the east side of Elm Street. The carrier notices that no two adjacent houses ever get mail on the same day, but that there are never more than two houses in a row that get no mail on the same day. How many different patterns of mail delivery are possible?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

9 Binomial Theorem, Pascal's Triangle, Combinatorial Identities

§9.1 Pascal's Triangle

Pascal's Triangle is a triangle generated by starting with the top row containing just 1. After that, each number is the sum of the two adjacent numbers in the row above it, with the left and right end of each row being 1. Above are the first 7 rows of Pascal's triangle. From now on, we'll refer to the top row as row 0, the second row as row 1, and so on.

$$\begin{array}{ccccccccccccc} & & & & & & 1 & & & & & & \\ & & & & & 1 & & 1 & & & & & \\ & & & & 1 & & 2 & & 1 & & & & \\ & & & 1 & & 3 & & 3 & & 1 & & & \\ & & 1 & & 4 & & 6 & & 4 & & 1 & & \\ & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \end{array}$$

There are numerous patterns in Pascal's triangle. For example, you might notice the sequence $1, 2, 3, \ldots$ in a diagonal. After some more observation, you might notice that the sum of the entries in each row is a power of 2. If you are very astute, you might even notice that if you sum the numbers in a left-pointing diagonal of any length, this sum is equal to the number directly below and to the right of where you ended the diagonal. We'll be exploring these patterns in this handout.

First, we'll start with an observation about binomials. When we expand $(x+1)^2$, we get x^2+2x+1. When we expand $(x+1)^3$ we get x^3+3x^2+3x+1. Do you notice anything?

The coefficients of the first expansion are 1, 2, and 1 in order. The coefficients of the second one are 1, 3, 3, and 1. These are precisely the third and fourth rows of Pascal's triangle! This works for $(x+1)^1 = x+1$ and $(x+1)^0 = 1$ as well. It turns out that it is true in the general case.

So far we have a connection between expansions of $(x+1)^n$ and the triangle. But we may also notice another strange pattern– every entry of Pascal's triangle is $\binom{n}{k}$ for some n and k. For instance, $1 = \binom{4}{0}$,0 $4 = \binom{4}{1}$, $6 = \binom{4}{2}$, $4 = \binom{4}{3}$ and $1 = \binom{4}{4}$. We can conjecture that row n has all numbers of the form $\binom{n}{i}$ for integers i between 0 and n inclusive, from left to right.

Exercise 9.1. Check this for the first 6 rows.

How do we prove this generally? We can use induction and the definition of Pascal's triangle. The first row is obvious to check.

Every number is the sum of the two above it. For the inductive step, assume our observation about binomial coefficients holds for $n-1$. We will show it holds for n.

An entry in position k in row n is $\binom{n}{k}$, and the numbers above it are $\binom{n-1}{k}$ and $\binom{n-1}{k-1}$. So we need to prove that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof. Let's prove this combinatorially. The LHS is the number of ways to choose k objects out of n objects. Directing our attention to one object, We consider two cases: if this object is in our group, we need to choose $k-1$ objects out of the $n-1$. This can be done in $\binom{n-1}{k-1}$ ways. If the object isn't in our group, we can choose k objects out of the other $n-1$, giving us the other $\binom{n-1}{k}$ ways, and we are done. ■

Exercise 9.2. Prove this algebraically by expanding out the binomials.

Now we have a nice description of Pascal's triangle. Furthermore, the fact that both numbers of the form $\binom{n}{k}$ and binomial expansions are connected to Pascal's triangle suggests a connection between these two objects. This connection is known as the **Binomial Theorem**.

§9.2 Binomial Theorem

The Binomial Theorem is a simple theorem that can be applied in numerous contexts in algebra and discrete math.

Theorem 9.3 (Binomial Theorem)**.** *For any positive integer n,*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n}y^n.$$

Proof. To prove the Binomial Theorem, we simply expand out the left hand side. That is, we write it as

$$(x+y)(x+y)\ldots(x+y).$$

Now say we need to find the coefficient of x^n. This is the number of ways we can choose n x's from the n brackets. But we can do this in only one way! Hence, the coefficient of x^n must be 1.

Now let's try and find the coefficient of $x^{n-1}y$. When we expand the above product, when will we get a $x^{n-1}y$? Of course, we need to choose a y in one of the binomials and an x in the rest.

In how many ways can we do this? The number of ways of choosing one y in n brackets is $\binom{n}{1}$. Looks like we are on the right track... can we generalise this argument? Let's try.

Let's say we want to find the coefficient of $x^{n-k}y^k$. We can get such a term iff we choose y's in k binomials and x in the rest. How many ways can we choose k of these binomials out of all n? Of course, in $\binom{n}{k}$ ways.

Thus, once we distribute on the LHS, we are simply adding together $\binom{n}{k}$ terms of each term of the form $x^{n-k}y^k$ for all integral k from 0 to n inclusive, giving us the result on the RHS, and we are done. ■

Exercise 9.4. Prove the Binomial Theorem using induction.

Exercise 9.5. What do you get when you substitute $x = y = 1$ into the Binomial theorem? How about $x = 1$, $y = -1$?

Example 9.6 (1963 AHSME). In the expansion of $\left(a - \frac{1}{\sqrt{a}}\right)^7$, what is the coefficient of $a^{-\frac{1}{2}}$?

Solution. Since we are expanding out the product of a binomial raised to a high power, the Binomial Theorem comes to mind. By the Binomial Theorem, each term of the expansion of $\left(a - \frac{1}{\sqrt{a}}\right)^7$ is of the form $\binom{7}{n} a^n \left(-\frac{1}{\sqrt{a}}\right)^{7-n}$. We want the coefficient of $a^{-\frac{1}{2}}$; in other words, we want

$$n + \left(-\frac{7}{2} + \frac{n}{2}\right) = -\frac{1}{2} \implies \frac{3}{2}n = 3 \implies n = 2.$$

Therefore, the coefficient of $a^{-\frac{1}{2}}$ is $(-1)^5 \cdot \binom{7}{2} = -21$. ■

This problem wasn't actually a counting problem, but it illustrates how we apply the Binomial Theorem.

Example 9.7 (2012 AMC 10B). Let $(a_1, a_2, \ldots a_{10})$ be a list of the first 10 positive integers such that for each $2 \le i \le 10$ either $a_i + 1$ or $a_i - 1$ or both appear somewhere before a_i in the list. How many such lists are there?

Solution. When we first look at this problem and test random numbers, we realize that the number of possibilities depends on what we choose for the first number. This motivates us to solve this problem using casework.

- The first number in the list is 1. Then, there is only one way to arrange the numbers (think about why this is true!), namely $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$.
- The first number in the list is 2. Then, we must pick one of the remaining spots to be 1, and the remaining spots will be filled up with 3, 4, 5... in that order. We can pick any of the 9 spots (other than the first one) to be the 1, so there are $\binom{9}{1}$ ways.
- The first number in the list is 3. Then, we must pick 2 of the remaining spots to be 2 and 1 (in that order!). We can pick any 2 of the 9 spots left, so there are $\binom{9}{2}$ ways.

$$\vdots$$

- The first number in the list is 10. Then, we must pick 9 of the 9 remaining spots to be the numbers 9, 8, 7, ..., 2, 1 in that order. There are $\binom{9}{9}$ ways to do this.

In total, we are trying to calculate

$$\binom{9}{0} + \binom{9}{1} + \cdots \binom{9}{9} = 2^9 = 512.$$

If you do not understand how we got to the final step, look at Exercise 9.5. ■

Example 9.8 (1993 AIME). Let S be a set with six elements. In how many different ways can one select two not necessarily distinct subsets of S so that the union of the two subsets

is S? The order of selection does not matter; for example, the pair of subsets $\{a, c\}$, $\{b, c, d, e, f\}$ represents the same selection as the pair $\{b, c, d, e, f\}$, $\{a, c\}$.

Solution. It seems really hard to pick both sets at the same time, so instead we will be selecting each set individually. Suppose that the first set contains x elements. Then, there are $\binom{6}{x}$ ways to select the first set (we can choose any x elements).

For the second set, we *have* to choose the $6 - x$ elements that aren't in the first set, but we can choose whether or not to have the x elements in the first set as well. This makes the total number of ways to pick the second set 2^x. Since $0 \leq x \leq 6$,

$$\sum_{x=0}^{6} \binom{6}{x} 2^x = (1+2)^6 = 729.$$

Make sure you understand why this is true! We may be tempted to put down 729 as our final answer, but remember that the order of the sets doesn't matter. We counted every case twice (other than the case when both sets are equal to $\{a, b, c, d, e, f\}$), so our final answer is $\frac{729-1}{2} + 1 = 364 + 1 = 365$. ■

The Binomial Theorem is very useful when simplifying calculations. Some things that may remind us of this theorem include the expansion of an expression to some power and the summation of a binomial with a fixed top value and a variable on the bottom. If you see any of these things, the Binomial Theorem should come to mind!

Exercise 9.9. Find another (similar) solution to Example 9.8 that does not involve the Binomial Theorem.

Exercise 9.10. In the expansion of $(ax + b)^{2000}$, where a and b are relatively prime positive integers, the coefficients of x^2 and x^3 are equal. Find $a + b$.

§9.3 Hockey-Stick Identity

The Hockey-Stick Identity is a combinatorial identity that is often used in math competitions. Even though it may not look particularly special, it can simplify many calculations.

Theorem 9.11 (Hockey-Stick Identity). *For nonnegative integers n, r such that $n \geq r$,*

$$\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}.$$

Proof. We can prove the Hockey-Stick Identity by using a counting argument. We'll count the number of ways to put a identical balls in b distinguishable boxes in two different ways. By stars and bars, we know that there are

$$\binom{a+b-1}{b-1}$$

ways to do this. However, we can also find this value using casework.

- If we put 0 balls into the first box, then there are $\binom{a+b-2}{b-2}$ ways to put the balls in the remaining boxes.

- If we put 1 ball into the first box, then there are $\binom{a+b-3}{b-2}$ ways to put the remaining balls in the remaining boxes.
- If we put 2 balls into the first box, then there are $\binom{a+b-4}{b-2}$ ways to put the remaining balls into the remaining boxes.

$$\vdots$$

- If we put a balls into the first box, then there are $\binom{a+b-2-a}{b-2}$ ways to put the remaining balls into the remaining boxes.

We know that we should get the same answer with both methods, so

$$\sum_{k=0}^{a} \binom{k+b-2}{b-2} = \binom{a+b-1}{b-1}.$$

If we let $r = b-2$, $n = a+b-2$, and $i = k+b-2$, then the above equation becomes

$$\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}.$$

■

Remark. The Hockey-Stick Identity gets its name from the fact that the values form a hockey stick on Pascal's Triangle. The LHS forms the "shaft" of the hockey stick and the RHS forms the "blade". For example, with $n = 5$ and $r = 2$, the hockey stick would like like this:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & \underline{\mathbf{1}} & & \\
 & 1 & & 3 & & \underline{\mathbf{3}} & & 1 & \\
1 & & 4 & & \underline{\mathbf{6}} & & 4 & & 1
\end{array}$$

Note that $1 + 3 + 6 + 10 = 20$.

Example 9.12 (2006 SMT)**.** Simplify:

$$\sum_{k=10}^{2006} \binom{k}{10}.$$

Your answer should contain no summations but may still contain binomial coefficients and/or combinations.

Solution. This problem is a very direct application of the Hockey-Stick identity with $n = 2006$ and $r = 10$. The answer is

$$\binom{2006+1}{10+1},$$

which is $\binom{2007}{11}$. ■

Example 9.13 (2013 AIME I). Melinda has three empty boxes and 12 textbooks, three of which are mathematics textbooks. One box will hold any three of her textbooks, one will hold any four of her textbooks, and one will hold any five of her textbooks. If Melinda packs her textbooks into these boxes in random order, the probability that all three mathematics textbooks end up in the same box can be written as $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m+n$.

Solution. You may remember this problem from the first day of combinatorics. This time, we'll solve it faster using the Hockey-Stick identity.

There are three possibilities for where the math books go. They could go in any of the three boxes, and the calculations will be different in each case, so we'll use casework.

- The math books are all in the smallest box (the one that holds 3 books). There are $\binom{3}{3}$ ways to do this.
- The math books are all in the middle box (the one that holds 4 books). There are $\binom{4}{3}$ ways to do this.
- The math books are all in the largest box (the one that holds 5 books). There are $\binom{5}{3}$ ways to do this.

Of course, we can calculate each value individually, but we can also simplify our calculations by using Hockey-Stick. This comes to mind because the top numbers of the binomials are consecutive integers and the bottom value is the same as the smallest of the top values. $\binom{3}{3}+\binom{4}{3}+\binom{5}{3}=\binom{6}{4}=\binom{6}{2}$. Our answer is

$$\frac{\text{number of ways to put all 3 math books in one box}}{\text{total number of ways to put 3 math books in the boxes}}=\frac{\binom{6}{2}}{\binom{12}{2}}=\frac{15}{220}=\frac{3}{44}.$$

Our desired value is $3+44=47$. ■

We will finish this section with a harder example.

Example 9.14 (2015 AIME I). Consider all 1000-element subsets of the set $\{1, 2, 3, \ldots, 2015\}$. From each such subset choose the least element. The arithmetic mean of all of these least elements is $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p+q$.

Solution. This problem may look very intimidating, so let's think about what it's asking for. We are asked to find the average of all the least elements, or

$$\frac{\text{sum of the least elements of all 1000-element subsets}}{\text{total number of distinct 1000-element subsets}}.$$

The denominator is fairly easy to find, it's just $\binom{2015}{1000}$, since we are choosing 1000 of the 2015 values to form a set. The numerator is a lot harder to find, because the smallest number varies with each subset. This motivates us to use casework.

- The smallest element of the subset is 1. There are $\binom{2014}{999}$ such subsets. (Why?)
- The smallest element of the subset is 2. There are $\binom{2013}{999}$ such subsets (since none of the other elements can be 1 or 2).

⋮

- The smallest element of the subset is 1016. There are $\binom{999}{999}$ such subsets (since none of the elements can be 1, 2, ..., 1015, or 1016).

Note that we cannot have a subset with 1017 as its smallest element, since the largest element we can have is 2015 and we must have 1000 distinct elements. The sum of the least elements of all 1000-element subsets is

$$1 \cdot \binom{2014}{999} + 2 \cdot \binom{2013}{999} + 3 \cdot \binom{2012}{999} + 4 \cdot \binom{2011}{999} + \ldots + 1016 \cdot \binom{999}{999}.$$

This value is very hard to compute by itself, but notice that we can split it up as follows:

$$\begin{aligned}
= &\binom{2014}{999} + \binom{2013}{999} + \binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} \\
&+ \binom{2013}{999} + \binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} \\
&+ \binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} \\
&+ \binom{2011}{999} + \ldots + \binom{999}{999} \\
&\vdots \\
&+ \binom{999}{999}
\end{aligned}$$

It is very hard to sum everything together, but it becomes much easier when we try to add the values one row at a time. By the Hockey-Stick Identity,

$$\begin{aligned}
\binom{2014}{999} + \binom{2013}{999} + \binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} &= \binom{2015}{1000} \\
\binom{2013}{999} + \binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} &= \binom{2014}{1000} \\
\binom{2012}{999} + \binom{2011}{999} + \ldots + \binom{999}{999} &= \binom{2013}{1000} \\
\binom{2011}{999} + \ldots + \binom{999}{999} &= \binom{2012}{999} \\
&\vdots \\
\binom{999}{999} &= \binom{1000}{1000}
\end{aligned}$$

We can simplify the sum to

$$\binom{2015}{1000} + \binom{2014}{1000} + \binom{2013}{1000} + \binom{2012}{1000} + \cdots \binom{1000}{1000}.$$

While this looks better than the first expression we got, it is still very hard to calculate. However, we can use the Hockey-Stick Identity one last time to compute the sum, which turns out to be $\binom{2016}{1001}$.

This may look like the answer, but remember that we are not done yet! We are asked for the expected value, which is

$$\frac{\binom{2016}{1001}}{\binom{2015}{1000}} = \frac{2016!}{1001!1015!} \cdot \frac{1000!1015!}{2015!} = \frac{2016}{1001} = \frac{288}{143}.$$

Once again, we are dividing by $\binom{2015}{1000}$ because that is the total number of distinct 1000-element subsets. The question asks for the sum of the numerator and the denominator, which is $288 + 143 = 431$. ■

We can take away a few things from this problem. First, if a problem seems too hard at first, try simplifying it into something that's easier or something that you can do. Second, sometimes it's worth changing perspectives when trying to simplify a value. Third, remember what you're looking for! Don't do everything correctly only to get it wrong because you didn't read the question.

In any problem involving a large sum of binomial coefficients, you should consider using Hockey-Stick, and see if you can manipulate the expression into a form where you can apply Hockey-Stick. When you are summing multiple binomial coefficients $\binom{n}{k}$ with constant k and consecutive n, remember this very important identity!

§9.4 Vandermonde's Identity

Similar to the Hockey-Stick Identity, Vandermonde's Identity can often be used to simplify answers and to get a cleaner solution.

Theorem 9.15 (Vandermonde's Identity)**.** *For nonnegative integers m, n, and r, where $r \leq m, n$,*

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}.$$

Proof. We will prove this theorem using a combinatorial argument; that is, we will show the left and right sides of the equation count the same thing.

First, let's try to figure out what the RHS could count. Obviously, we could say we are choosing a set of r people out of $m + n$. What will m and n represent?

Let's suppose there are m boys and n girls, and we are trying to form a team of r from this group. The RHS clearly describes this. How about the LHS? Let's try looking at a single term in the sum, say, $\binom{m}{2}\binom{n}{r-2}$. What does this mean?

The first term is equivalent to the number of ways of choosing 2 out of m boys, and the second counts the number of ways to choose $r - 2$ out of the n girls. This forms a team of r, but with a specific number of boys and girls. But in the RHS, the number of boys and girls could be anything.

That's why we're summing these single terms over all possible values of k in the LHS! The first term is the number of ways of choosing a team of r girls, the second is the number of ways of choosing $r - 1$ girls and 1 boy, and so on, with the last term being the number of ways of choosing r boys in the team. In total, this covers each and every way to choose a team of r from a pool of n girls and m boys, which is exactly what the RHS counts as well, and we are done. ■

Make sure you fully internalize and understand the above proof; it is a classic example of a combinatorial argument.

Example 9.16. Prove that

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Solution. This identity looks extremely similar to Vandermonde's Identity because of the summation from 0 to n and the product of two binomials, so we'll try to apply it. When we substitute $n = m = r$ into Vandermonde's, we get

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}.$$

We know that $\binom{n}{k} = \binom{n}{n-k}$, so we are done. ■

Example 9.17 (2020 AIME I). A club consisting of 11 men and 12 women needs to choose a committee from among its members so that the number of women on the committee is one more than the number of men on the committee. The committee could have as few as 1 member or as many as 23 members. Let N be the number of such committees that can be formed. Find the sum of the prime numbers that divide N.

Solution. Suppose that we pick k men and $k+1$ women to be on the committee. k ranges from 0 to 11, so the total number of ways to do choose a committee is

$$\binom{11}{0}\binom{12}{1} + \binom{11}{1}\binom{12}{2} + \cdots \binom{11}{11} + \binom{12}{12},$$

which is

$$\sum_{k=0}^{11} \binom{11}{k}\binom{12}{k+1} = \sum_{k=0}^{11} \binom{11}{k}\binom{12}{12-(k+1)} = \sum_{k=0}^{11} \binom{11}{k}\binom{12}{11-k}.$$

Once again, the product of the binomials reminds us of Vandermonde's. When we compare Vandermonde's Identity to this expression, we see that this is Vandermonde's when $m = 11, n = 12$, and $r = 11$, so the number of ways is

$$\binom{11+12}{11} = \binom{23}{11} = 2 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23.$$

Thus, the answer is $2 + 7 + 13 + 17 + 19 + 23 = 81$. ■

Vandermonde's Identity is used when we are trying to find the sum of the product of two binomials. In the majority of cases involving the product of two binomials, Vandermonde's Identity can make the calculation much easier.

§9.5 Homework Problems

Problem 9.1. [3] Given $(x+y)^{10}$, find the coefficient of the x^4y^6 term.

Problem 9.2 (1975 AHSME). [5] What is the smallest integer larger than $(\sqrt{3}+\sqrt{2})^6$?

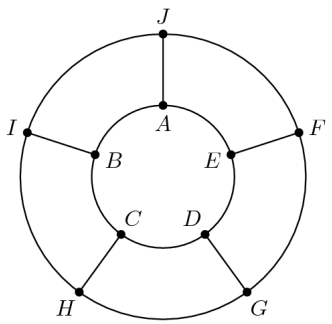
Problem 9.3 (2001 AIME I)**.** [6] Find the sum of the roots, real and non-real, of the equation $x^{2001} + \left(\frac{1}{2} - x\right)^{2001} = 0$, given that there are no multiple roots.

Problem 9.4 (1992 AIME)**.** [7] In Pascal's Triangle, each entry is the sum of the two entries above it. In which row of Pascal's Triangle do three consecutive entries occur that are in the ratio $3 : 4 : 5$?

Problem 9.5 (2016 AMC 10A)**.** [7] For some particular value of N, when $(a+b+c+d+1)^N$ is expanded and like terms are combined, the resulting expression contains exactly 1001 terms that include all four variables a, b, c, and d, each to some positive power. What is N?

Problem 9.6 (2008 iTest)**.** [6] Find the sum of the 2007 roots of $(x-1)^{2007} + 2(x-2)^{2006} + 3(x-3)^{2005} + \cdots + 2006(x-2006)^2 + 2007(x-2007)$.

Problem 9.7 (2018 AIME I)**.** [9] The wheel shown below consists of two circles and five spokes, with a label at each point where a spoke meets a circle. A bug walks along the wheel, starting at point A. At every step of the process, the bug walks from one labeled point to an adjacent labeled point. Along the inner circle the bug only walks in a counterclockwise direction, and along the outer circle the bug only walks in a clockwise direction. For example, the bug could travel along the path $AJABCHCHIJA$, which has 10 steps. Let n be the number of paths with 15 steps that begin and end at point A. Find the remainder when n is divided by 1000.



Hint: Consider a sequence of moves as a string, where an I represents a clockwise movement (in the inner circle), an O represents a counterclockwise movement (in the outer circle), and an S represents a switch between the inner and outer circle. What do we know about the number of Is and Os?

Problem 9.8 (2006 AIME II)**.** [9] Seven teams play a soccer tournament in which each team plays every other team exactly once. No ties occur, each team has a 50% chance of winning each game it plays, and the outcomes of the games are independent. In each game, the winner is awarded a point and the loser gets 0 points. The total points are accumulated to decide the ranks of the teams. In the first game of the tournament, team A beats team B. The probability that team A finishes with more points than team B is m/n, where m and n are relatively prime positive integers. Find $m+n$.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

10 Probability

Today, we'll review probability. It won't be very different from previous handouts this week because many probability problems are just counting problems in disguise.

We can define **probability** of a certain event as the number of outcomes where the event occurs (assuming all outcomes have equal probability) over the total possible number of outcomes. We can also think of it as the proportion of times an event will occur if we repeat a certain process many times.

For example, the probability a fair coin flips heads is $\frac{1}{2}$. There are two outcomes, heads and tails, with equal probability.

§10.1 Independent/Dependent Events

A pitfall in probability problems is failing to recognize when events are independent and when they are dependent. To avoid making this mistake, let's define these two terms and work through some related problems.

Definition 10.1. Two events are **independent** if the outcome of one event does not affect the outcome of the other.

Let X and Y be two events. We let $P(X)$ denote the probability of event X occurring. We denote the probability that X and Y both occur as $P(X \cap Y)$.

Proposition 10.2 (Independent Events). *Assume we have two independent events A and B. Then $P(A \cap B) = P(A) \cdot P(B)$.*

Exercise 10.3. Prove this using the definition of an independent event.

.

Example 10.4. I roll two fair dice numbered $1, 2, 3 \ldots, 6$. What is the probability that I roll two 1s?

Solution. In this problem, the outcome of each roll is independent because the result of our first roll does not affect the result of the second roll. The probability that a single die shows 1 is $\frac{1}{6}$. Thus, the probability that both dice show 1 is $\left(\frac{1}{6}\right)\left(\frac{1}{6}\right) = \frac{1}{36}$. ■

This problem was a pretty simple, yet constructive example of independent events. If two events are independent, we can calculate the probability that each event happens individually and multiply them to find the probability that they both happen.

Example 10.5. I roll two fair dice numbered 1 through 6. What is the probability that I roll at least one 1?

Solution. We can use the ideas of complementary counting here. Let's calculate the probability that we roll no 1s instead. The probability that one dice does not roll as 1 is $\frac{5}{6}$. Then the

probability that both dice don't show 1 is $\frac{25}{36}$. Thus, the probability that at least one die rolls 1 is $1 - \frac{25}{36} = \frac{11}{36}$. ■

Example 10.6. We roll 3 dice numbered 1 through 6. What is the probability that exactly one die rolls 1?

Solution. The probability that one die rolls 1 is $\frac{1}{6}$, and the probability that the other two do not roll 1 is $\frac{5}{6}$. Since there are 3 choices for the die that rolls 1, our desired probability is $3(\frac{1}{6})(\frac{5}{6})^2 = \frac{75}{216}$. ■

Independent events are relatively straightforward. The general idea is: find the probabilities of the events who want(or don't want in the case of complementary probability), and multiply them together. As we will see, dependent probability is a lot more complicated because, as the name suggests, events depend on the outcome of other events which adds a whole new wrinkle in the problem.

Definition 10.7. Two events are **dependent** if the outcome of one event affects the outcome of the other event (i.e. change the probability it occurs).

Example 10.8. I shuffle a standard deck of 52 cards and deal them. What is the probability that the first two cards I deal are spades?

Solution. These events are dependent because after the first spade is dealt, it is removed from the deck, lowering the probability of drawing a second spade. The probability that the first card is a spade is $\frac{13}{52} = \frac{1}{4}$. Since there are now 12 spades remaining out of the 51 undealt cards, the probability that the second card is a spade is $\frac{12}{51} = \frac{4}{17}$. Thus, the probability that the first two cards dealt are spades is $\left(\frac{1}{4}\right)\left(\frac{4}{17}\right) = \frac{1}{17}$. ■

It is important to note the difference between "with replacement" and "without replacement". When we talk about doing something with replacement, it means we are resetting the event each time. When we talk about doing something without replacement, it's the opposite: each event's change on the outcome of the next event is permanent.

Example 10.9. I have a hat with 10 slips of paper numbered 1 through 10. What is the probability that I draw a 1?

1. With replacement
2. Without replacement

Solution.
Let's first consider the problem with replacement. Since we are choosing numbers with replacement, we can think of this as rolling a 10 sided die. There is a $\frac{1}{10}$ chance that we draw a one on any given draw. It follows that the probability we don't draw a 1 is $(\frac{9}{10})^3 = \frac{729}{1000}$. Thus, the probability that we draw a 1 is $\frac{271}{1000}$

For the second part, we can use the same idea, but we must remember that we are choosing numbers without replacement. The probability that our first draw is not 1 is $\frac{9}{10}$. Since we do not replace the number we drew, the probability that our second draw is not 1 is $\frac{8}{9}$. Similarly,

the probability that our third draw is not 1 is $\frac{7}{8}$. Thus, the probability that we draw a 1 is $1-(\frac{9}{10})(\frac{8}{9})(\frac{7}{8})=1-\frac{7}{10}=\frac{3}{10}$. ■

Now let's move on to some more complicated problems involving independent and dependent events.

Example 10.10 (AMC 12). A coin is biased in such a way that on each toss the probability of heads is $\frac{2}{3}$ and the probability of tails is $\frac{1}{3}$. The outcomes of the tosses are independent. A player has the choice of playing Game A or Game B. In Game A she tosses the coin three times and wins if all three outcomes are the same. In Game B she tosses the coin four times and wins if both the outcomes of the first and second tosses are the same and the outcomes of the third and fourth tosses are the same. How do the chances of winning Game A compare to the chances of winning Game B?

Solution. This problem is wordy, but we are essentially solving for and comparing two different probabilities. Since we are flipping coins, each outcome is separate from another and thus independent(the problem also tells us this).

The probability that we win Game A is just $\left(\frac{2}{3}\right)^3+\left(\frac{1}{3}\right)^3=\frac{9}{27}=\frac{1}{3}$.

Calculating the probability that we win Game B is a little trickier. There are 4 possible winning outcomes: HHTT, HHHH, TTHH, TTTT. Thus, the probability that we win Game B is $\left(\frac{2}{3}\right)^2\left(\frac{1}{3}\right)^2+\left(\frac{2}{3}\right)^2\left(\frac{2}{3}\right)^2+\left(\frac{1}{3}\right)^2\left(\frac{2}{3}\right)^2+\left(\frac{1}{3}\right)^2\left(\frac{1}{3}\right)^2=\frac{25}{81}$.

Thus, the probability that we win Game A is $\frac{2}{81}$ higher than the probability that we win Game B. ■

Finding the probability that we won Game A was a pretty straightforward application of what we know about independent events, and it just took some extra casework to find the probability for Game B.

Example 10.11 (AIME). An urn contains 4 green balls and 6 blue balls. A second urn contains 16 green balls and N blue balls. A single ball is drawn at random from each urn. The probability that both balls are of the same color is 0.58. Find N.

Solution. We have two cases that are successful: either both balls drawn are green or both are blue.

Case 1: Both balls drawn are green

Notice that we are dealing with independent events here because one green ball being drawn from the first urn does not affect the probability of a green ball being drawn from the second as the urns are separate. The probability that the ball from the first urn is green is $\frac{4}{4+6}=\frac{2}{5}$. The probability that the ball from the second urn is green is $\frac{16}{16+N}$. Thus, the probability that both balls drawn are green is $\left(\frac{2}{5}\right)\left(\frac{16}{16+N}\right)=\left(\frac{32}{80+5N}\right)$.

Case 2: Both balls drawn are blue

Using similar logic, the probability that the ball from the first urn is blue is $\frac{6}{10}=\frac{3}{5}$. The probability that the ball from the second urn is blue is $\frac{N}{16+N}$. Thus, the probability that both

balls are blue is $\left(\frac{3}{5}\right)\left(\frac{N}{16+N}\right) = \left(\frac{3N}{80+5N}\right)$.

Summing up the two cases, we have that the total probability that both balls chosen are the same color is $\frac{32+3N}{80+5N} = \frac{58}{100} = \frac{29}{50}$. Cross multiplying, we get $1600 + 150N = 2320 + 145N$, so $N = 144$. ■

Now let's take a look at a problem involving dependent probability.

Example 10.12 (Mathcounts). A $3 \times 3 \times 3$ wooden cube is painted on all six faces, then cut into 27 unit cubes. One unit cube is randomly selected and rolled. After it is rolled, 5 of the 6 faces of the cube are visible. What is the probability that exactly one of the 5 visible faces is unpainted?

Solution. Observe that when we cut the cube, some unit cubes will have 1 painted face, some will have 2, some will have 3, and the one cube in the middle will have 0 painted faces. If we visualize the cube, we find that the 8 corners all have 3 painted faces, the 12 cubes in between the corners have 2 painted faces, the 6 cubes in the center of each face have 1 painted face, and the cube in the middle has no painted faces.

Notice that it is impossible for exactly one visible face to be painted with the 0 painted face cube because it literally has 0 painted faces, and it is also impossible for the cube with 3 painted faces because at least two visible faces are always painted.

The solutions lie in the other two possible cubes. If we pick a cube with exactly 1 painted face, then the hidden face can not be the originally painted face. Since there is a $\frac{6}{27}$ probability that we even choose this type of cube in the first place, there is a $\frac{6}{27} \cdot \frac{5}{6} = \frac{5}{27}$ probability of success in this scenario. If we pick a cube with exactly 2 painted faces, then the hidden face must be an originally painted face. Since there were 12 of these cubes to start with, we have a $\frac{12}{27} \cdot \frac{2}{6} = \frac{4}{27}$ chance of success in this case.

Thus, the probability that exactly one of the 5 visible faces is painted is $\frac{5}{27} + \frac{4}{27} = \frac{1}{3}$. ■

Exercise 10.13. I roll three dice. What is the probability that the numbers rolled on two of the dice sum to the third?

Exercise 10.14. Six people each flip a fair coin. Everyone who flipped tails then flips their coin again. Given that the probability that all the coins are now heads can be expressed as simplified fraction $\frac{m}{n}$, compute $m + n$.

Exercise 10.15. When rolling a certain unfair six-sided die with faces numbered 1, 2, 3, 4, 5, and 6, the probability of obtaining face F is greater than 1/6, the probability of obtaining the face opposite is less than 1/6, the probability of obtaining any one of the other four faces is 1/6, and the sum of the numbers on opposite faces is 7. When two such dice are rolled, the probability of obtaining a sum of 7 is 47/288. Find the probability of rolling face F.

§10.2 Conditional Probability

Definition 10.16. The **conditional probability** of an event A given another event B is the probability that A occurs given that B occurs. We denote this probability as $P(A|B)$.

We also denote the probability that both event A and event B occur as $P(A \cap B)$.

Proposition 10.17 (Conditional Probability). $P(A|B) = \frac{P(A \cap B)}{P(B)}$.

If this doesn't make sense at first, think of it in terms of words instead of notation. The probability that event A occurs given that event B occurs is the probability that both events A and B occur, divided by the probability that event B occurs.

Compared with traditional probability, the main difference with conditional probability is that there is usually some restriction given that limits the possible outcomes.

Example 10.18. I roll two fair dice, each numbered $1, 2, \ldots, 12$. Given that the first die rolls 11, what is the probability that the other die also rolls a prime number?

Solution. The first die roll does not influence the second die roll. As there are 5 primes (2, 3, 5, 7, 11) below 12, the probability that the second die rolls a prime is $\frac{5}{12}$. ■

Note that $P(A|B)$ for independent events A, B is simply $P(A)$ because forcing B to be true does not do anything for A. This logic can't apply for dependent events because the outcome of B affects the outcome of A.

$P(A|B)$ for dependent events A, B can be thought of as the number of ways for A and B to happen divided by the total number of ways for B.

Example 10.19. I have a fair six sided die. Given that the result is odd, what is the probability that

a) I rolled a 1

b) I rolled a prime number?

Solution. Let's consider both situations.

a) We are given that our result was odd, so we must have rolled a 1,3, or 5. All of these are equally likely, so the probability we rolled a 1 is $\frac{1}{3}$.

b) Out of the three possible outcomes of 1,3, and 5, both 3 and 5 are prime. Thus, the probability that we roll a prime is $\frac{2}{3}$. ■

Let's take a look at another problem continuing with the team of rolling dice.

Example 10.20. I roll two fair six sided dice. Given that at least one of the dice rolls 2, what is the probability that the sum of the two dice is 5?

Solution. Let's begin by first counting the number of possible outcomes with the restriction.

There are 6 outcomes for the second die when we roll the first die as 2 and also 6 outcomes for the first die when we roll the second die as 2. There is also one outcome where we roll two 2s. Thus, by PIE, the number of possible outcomes is $6 + 6 - 1$ or 11.

Now, we need to count our successful outcomes. The only possible successes are rolling a $2, 3$ or a $3, 2$. Thus, the desired probability is $\frac{2}{11}$. ■

Exercise 10.21 (AHMSE). A fair standard six-sided dice is tossed three times. Given that the sum of the first two tosses equal the third, what is the probability that at least one 2 is tossed?

Example 10.22 (AIME). There is a 40% chance of rain on Saturday and a 30% chance of rain on Sunday. However, it is twice as likely to rain on Sunday if it rains on Saturday than if it does not rain on Saturday. The probability that it rains at least one day this weekend is $\frac{a}{b}$, where a and b are relatively prime positive integers. Find $a+b$.

Solution. Let x be the probability that it rains on Sunday given that there is no rain on Saturday. Then, we have that

$$\frac{2}{5}(2x)+\frac{3}{5}x=\frac{3}{10} \implies x=\frac{3}{14}.$$

So the probability that it doesn't rain on Sunday given that it doesn't rain on Saturday is $\frac{11}{14}$. Since we already know the probability that it doesn't rain on Saturday, the probability that it doesn't rain both days is $\frac{11}{14}\cdot\frac{3}{5}=\frac{33}{70}$. Thus, the probability that it rains at least one day is $\frac{37}{70}$, and our desired sum is 107. ■

Here's another example:

Example 10.23. I'm planning a party. Kevin says he has a 80% chance of showing up. Russell tells me he has a 30% chance of going if Kevin is going. Otherwise, he has a 75% chance of showing up. If I see Russell, what is the probability Kevin is also there?

Solution. The probability that both Kevin and Russell are at my party is $\frac{8}{10}\cdot\frac{3}{10}=\frac{3}{25}$. The probability that just Russell is there is $\frac{2}{10}\cdot\frac{3}{4}=\frac{3}{20}$.

Thus, the probability that Kevin is at the part given that Russell is also there is $\frac{\frac{3}{25}}{\frac{3}{25}+\frac{3}{20}}=\frac{12}{27}$. ■

Exercise 10.24. 2 percent of the population of America have contracted a certain type of disease. Fortunately, a screening test for the disease has been developed that claims to be 95 percent accurate"; that is, the test will return the correct results in 95 percent of the cases and return incorrect results in the other 5 percent of the cases. What is the probability that someone tested positive for the virus actually has the virus(calc allowed)?

Let's move on to a more complicated problem.

Example 10.25 (HMMT). Urn A contains 4 white balls and 2 red balls. Urn B contains 3 red balls and 3 blackballs. An urn is randomly selected, and then a ball inside of that urn is removed. We then repeat the process of selecting an urn and drawing out a ball, without returning the first ball. What is the probability that the first ball drawn was red, given that the second ball drawn was black?

Solution. We first count the probability where a black ball is the second ball drawn and then find the intersection for when a red ball then black ball is drawn. Dividing our first result by our second, we will get our desired probability.

To find the probability where a black ball is chosen second, we have three cases: a ball was chosen from urn A first(color doesn't matter), a red ball was chosen from urn B, or a black ball was chosen from urn B.

Case 1: Ball from Urn A first

This probability is $\frac{1}{2} \cdot 1 \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$.

Case 2: Red ball from Urn B first

This probability is $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{5} = \frac{3}{40}$.

Case 3: Black ball from Urn B first

This probability is $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{5} = \frac{2}{40}$

Thus, the probability a black ball is chosen second is $\frac{1}{8} + \frac{3}{40} + \frac{2}{40} = \frac{1}{4}$.

Now, we just have to find the probability that a red ball was drawn first with a black ball being the second draw. There are two scenarios we need to consider. The first is when a red ball is drawn out of Urn A first, and the second is when a red ball is drawn out of Urn B first. The probability is $\frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{5} = \frac{1}{24} + \frac{3}{40} = \frac{7}{60}$.
Thus, the probability the first ball drawn was red given that the second ball drawn was black is $\frac{\frac{7}{60}}{\frac{1}{4}} = \frac{7}{15}$. ■

This seemed to be a pretty confusing problem at first glance, but it essentially boiled down to applying the formula we introduced at the beginning of the section. However, don't think of it as a formula, it should come naturally. The probability that event B happens can be thought of as the possible outcomes and the probability that both occur can be thought of as successful outcomes. When you think about it, our formula for conditional probability is no different than traditional probability!

> *Remark.* The Monty Hall Problem is a fun application of conditional probability. The problem goes:
>
> Suppose you're on a game show, and you're given the choice of three doors: Behind one door is a car; behind the others, goats. You pick a door, say No. 1, and the host, who knows what's behind the doors, opens another door, say No. 3, which has a goat. He then says to you, Do you want to pick door No. 2? Is it to your advantage to switch your choice?
>
> Think about it!

Exercise 10.26 (AIME). Arnold is studying the prevalence of three health risk factors, denoted by A, B, and C, within a population of men. For each of the three factors, the probability that a randomly selected man in the population has only this risk factor (and none of the others) is 0.1. For any two of the three factors, the probability that a randomly selected man has exactly these two risk factors (but not the third) is 0.14. The probability that a randomly selected man has all three risk factors, given that he has A and B is $\frac{1}{3}$. The probability that a man has none of the three risk factors given that he does not have risk factor A is $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p + q$.

Exercise 10.27 (AMC 10). Two counterfeit coins of equal weight are mixed with 8 identical genuine coins. The weight of each of the counterfeit coins is different from the weight of each of the genuine coins. A pair of coins is selected at random without replacement from the 10

coins. A second pair is selected at random without replacement from the remaining 8 coins. The combined weight of the first pair is equal to the combined weight of the second pair. What is the probability that all 4 selected coins are genuine?

§10.3 Geometric Probability

In probability, we occasionally are given problems where there's no way we can count the number of possibilities; there are infinitely many.. . .

Geometric probability is our solution. Instead of counting individual items, we represent our counts with geometric regions. Our desired probability is then given as the size of the region that represents a "success" divided by the size of the total region.

Let's take a look at an example.

Example 10.28. Segment $\overline{AB}$ has length 3. Let point C lie on $\overline{AB}$ with $AC = 2$. What is the probability a randomly chosen point is closer to C than A?

Solution. To begin, we have to ask ourselves what the successful region is. Let us denote D as the midpoint of AC. Notice that all points to the right of C are closer to C than A. $DB = 2$ and $AB = 3$.

Thus, the probability the point is closer to C than A is $\frac{2}{3}$. ■

Exercise 10.29. Let x be a real number in the range [-2, 2]. What is the probability $x^2 < 3$?

We can use geometric probability in two dimensions as well.

Example 10.30. Suppose you are playing a game in which you throw a dart at a circle of diameter 1 inscribed in a 1×1 square board. You win only if the dart hits the circle. What's the probability you win?

Solution. In this problem, our successful region is the circle and the total region is the square.

The area of the circle is $\frac{1}{4}\pi$ and the area of the square is 1. Thus, the probability the dart lands in the circle and we win is $\frac{1}{4}\pi$ ■

Now let's move on to a classic problem involving geometric probability.

Example 10.31. Anna and Bob are hoping to meet for lunch. They will each arrive at the restaurant sometime between 2 p.m. and 3 p.m., stay for 15 minutes, and then leave. What is the probability that they will meet each other at the restaurant?

Solution. There are infinitely many times that Bob and Anna could show up, so it makes sense to think of geometric probability.

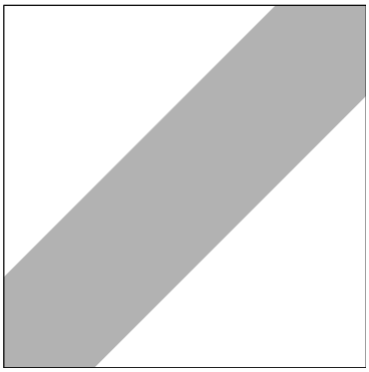
Let's set up a graph to represent the situation. Take the xy plane. We can let the x-axis represent the time Anna arrives, and we can let the y-axis represent the time Bob arrives.

Our total area of possibility can be as a square with side lengths of 60(for each minute in the hour).

Let's consider the successful region in terms of when Anna arrives. If Anna arrives at 2:00, Bob has until 2:15 to show up. If Anna arrives at 2:05, Bob has until 2:20 to show up and

he also could be waiting from possibly 2:00. If Anna arrives at 2:15, Bob could have arrived anytime between 2:00-2:30.

If we graph the successful regions, we notice that the successful region appears to be a hexagon and the unsuccessful region consists of two right isosceles triangles. The side lengths of both



triangles are 45, so our unsuccessful region has area $2\left(\frac{1}{2}\cdot 45\cdot 45\right) = 2025$. Thus, our successful region has area 1575 and our desired probability is $\frac{1575}{3600} = \frac{7}{16}$. ■

This is a pretty useful strategy for dealing with geometric probability problems. We may not know the shape at first, but by testing values, we can get a general idea of it and reason out the actual shape.

Example 10.32 (AMC 10). Chloe chooses a real number uniformly at random from the interval $[0, 2017]$. Independently, Laurent chooses a real number uniformly at random from the interval $[0, 4034]$. What is the probability that Laurent's number is greater than Chloe's number?

Solution. Similar to the previous problem, we can model this with the xy plane. Let the x-axis represent Laurent's number and let the y-axis represent Chloe's number. We have a rectangle with length 4034 and height 2017. Since Laurent's number is the x coordinate of whatever point is in the rectangle, our successful region is the intersection between the region $x > y$ and the rectangular region.

After graphing it, we notice that the area of the complement of our region is $\frac{2017\cdot 2017}{2}$, and the total area is $2017 \cdot 4034$. Thus, our desired probability is $1 - \frac{1}{4} = \frac{3}{4}$. ■

In conclusion, we want to use geometric probability when there's no way to individually count our successes. However, the basic idea of traditional probability remains: we find the area representing the possibilities we want, and divide by the total area.

Exercise 10.33. Nate and Francis go to the county carnival at a random time between noon and 6 PM. Nate stays for 2 hours and Francis stays for 3. What is the probability that they meet?

Exercise 10.34 (AMC). What is the probability that if three points are chosen at random on the circumference of a circle, then the triangle formed by connecting the three points does not have a side length greater than the radius?

§10.4 Homework Problems

Problem 10.1. [3] Bill is choosing cards out of a standard deck of 52 cards. Given that the first card is black, the probability that the second card is red can be expressed as $\frac{m}{n}$ where m

and n are relatively prime positive integers. Find $m+n$

Problem 10.2. [4] I roll one fair die and flip 6 coins. The probability that the number of times I get heads is equal to the number I roll on the dice can be expressed as $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m+n$.

Problem 10.3. [5] Andrew has an urn with 17 marbles, 3 are green, 4 are blue, 5 are red, and 5 are brown. Bill keeps taking marbles out of the urn until there are none left. The probability the 6th marble he chooses is blue can be expressed as $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m+n$

Problem 10.4. [5] Two points are chosen on a unit circle. The probability the distance between those two points is greater than 1 can be expressed as $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m+n$.

Problem 10.5. [5][2020 AMC 10/12B] An urn contains one red ball and one blue ball. A box of extra red and blue balls lie nearby. George performs the following operation four times: he draws a ball from the urn at random and then takes a ball of the same color from the box and returns those two matching balls to the urn. After the four iterations the urn contains six balls. The probability that the urn contains three balls of each color can be expressed as $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m+n$.

Problem 10.6. [6] A bag has 6 red marbles and 4 green marbles, another bag has 5 blue marbles and 4 green marbles. Jaedon first chooses one of the two bags at random, then chooses 2 marbles from the bag one at a time. If the first of the two marbles he chose was green, the probability the second marble he chooses is also green can be expressed as $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m+n$.

Problem 10.7. [6] Connor flips an unfair coin. The probability that Connor flips exactly 2 heads in 3 flips is equal to the probability that Connor flips exactly 3 tails in 4 flips. The probability the coin flips heads in 1 flip can be expressed as $\frac{p-\sqrt{q}}{r}$ p and r are relatively prime and q is not divisible by the square of any prime. Find $p+q+r$.

Problem 10.8. [7] [2017 AIME II] A triangle has vertices $A(0,0)$, $B(12,0)$, and $C(8,10)$. The probability that a randomly chosen point inside the triangle is closer to vertex B than to either vertex A or vertex C can be written as $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p+q$.

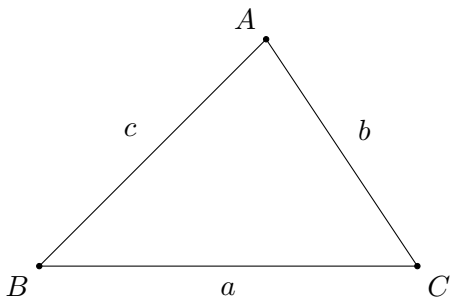
Problem 10.9. [7] [2017 AIME I] A circle is circumscribed around an isosceles triangle whose two congruent angles have degree measure x. Two points are chosen independently and uniformly at random on the circle, and a chord is drawn between them. The probability that the chord intersects the triangle is $\frac{14}{25}$. Find the difference between the largest and smallest possible values of x.

Problem 10.10. [7] [2017 AIME I] Two real numbers a and b are chosen independently and uniformly at random from the interval $(0,75)$. Let O and P be two points on the plane with $OP=200$. Let Q and R be on the same side of line OP such that the degree measures of $\angle POQ$ and $\angle POR$ are a and b respectively, and $\angle OQP$ and $\angle ORP$ are both right angles. The probability that $QR \leq 100$ is equal to $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m+n$.

11 Triangles I

§11.1 Introduction to Triangles

A **triangle** is a three-sided polygon. It is composed of three sides that together form three angles (hence why it is referred to as "tri-angle").



Throughout this week, in a triangle $\triangle ABC$ with vertices A, B, C, we will use the notation a, b, and c for the lengths of segments BC, CA, and AB, respectively. There are several types of special triangles. Note that a triangle can fit into multiple types here.

1. Equilateral: This one has three sides of equal length, and consequently, three angles of degree measure $60°$
2. Isosceles: This one has two sides of equal length. There is some debate about whether it should have exactly two equal sides or just at least two, but that will always be clarified on competitions. It has two equal base angles and one vertex angle.
3. Scalene: None of the side lengths or angles are equal to each other.
4. Acute: All angles are less than $90°$. All of these angles are namely **acute**.
5. Obtuse: One angle is greater than $90°$. This angle is namely the **obtuse** angle.
6. Right: One angle is exactly $90°$. The side opposite this **right angle** is the **hypotenuse**, which is also the longest side. The other two sides are called **legs**.

It is important to note that the first three types deal with side lengths whereas the last three deal with angles, thus creating the potential for overlap.

There are some restrictions on the side lengths of a triangle. If I asked you to create a triangle with lengths $2, 3$, and 5, you wouldn't be able to do it. At best, you would get a straight line because the smaller two side lengths add to get the third, creating a $180°$ angle. (A triangle like this is called **degenerate**). You need a set of lengths that connect to each other and enclose some non-zero area.

Theorem 11.1 (Triangle Inequality). *If a, b, and c are the side lengths of a triangle, then they must satisfy*

$$a + b > c$$

$$a + c > b$$

$$b + c > a.$$

Simply put, any one side has to be less than the sum of the other two. In order to find the range of acceptable values of the third side given the first two sides, just figure out two values for which the triangle is degenerate.

Example 11.2. There exists a triangle with side lengths 2, 3, and an unknown side. If I roll a fair 6 sided die, what is the probability that it can be used as the third side and form a non-degenerate triangle?

Solution. What values could the 3rd side length have to turn the triangle into a straight line? Well, if we subtract the lengths, we get $3-2=1$ as a lower bound and if we add them, we get $3+2=5$ as an upper bound. This means that we can have any length in the interval $(1,5)$ (excluding the endpoints).

Since 1 and 5 cannot be the side lengths, we can only consider the numbers between them as side lengths, namely $2, 3$, and 4. Since these are three numbers on the die, there is a $\frac{1}{2}$ chance that a die roll will give a valid side length. ■

Although it may be called the Triangle Inequality, this inequality extends to n-sided polygons in such a way that the sum of the smallest $n-1$ side lengths must be larger than the length of the longest side. You can use the same intuition about forming a line to understand why.

Example 11.3 (2017 AMC 10A). Joy has 30 thin rods, one each of every integer length from 1 cm through 30 cm. She places the rods with lengths 3 cm, 7 cm, and 15 cm on a table. She then wants to choose a fourth rod that she can put with these three to form a quadrilateral with a positive area. How many of the remaining rods can she choose as the fourth rod?

Solution. What rod values would make this quadrilateral a straight line?

Let's start by adding all of the three side lengths together. This gives an upper bound of 25. Furthermore, if we subtract the smaller two side lengths from the largest one, we get a lower bound of $15-3-7=5$. Thus, the fourth side length must be between 5 and 25 exclusive. There are 19 such values.

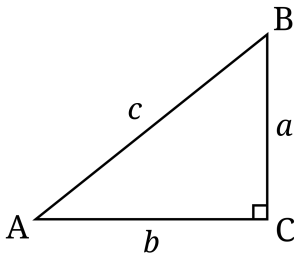
You may think that we are finished here. However, note that although 7 and 15 are part of this set of acceptable side lengths, they can't be the fourth side length since they are already used as one of the first three side lengths. and Joy only has one of each, so no repetitions are allowed. Thus the answer is $19-2=17$. ■

§11.2 Right Triangles

There turns out to be a more specific relationship between the side lengths of a right triangle beyond the Triangle Inequality.

Theorem 11.4 (Pythagorean Theorem). *Given any right triangle with leg lengths a, b and hypotenuse length c, we have*

$$a^2+b^2=c^2.$$



There are a multitude of ways to prove this, many of which you've probably seen. We'll ask you to prove this later in the handout.

A **Pythagorean triple** is a set of three integer values that form the sides of a right triangle. For example, 3-4-5 is a Pythagorean triple because

$$3^2 + 4^2 = 5^2$$

is true, so there exists a right triangle with legs of length 3, 4 and a hypotenuse of length 5.

It helps to know some smaller Pythagorean triples as because it may save calculation time and allow you to quickly recognize a right triangle in certain problems.

Example 11.5. Find some other Pythagorean triples with integer values less than 100.

Solution. Through inspection, we find some Pythagorean triples including, but not limited to, the following:

$$\begin{aligned}
&3-4-5\\
&6-8-10\\
&5-12-13\\
&8-15-17\\
&7-24-25\\
&9-40-41\\
&10-24-26\\
&20-21-29.
\end{aligned}$$

■

There are a few things worth noting:

- If a-b-c is a Pythagorean triple, then na-nb-nc is one as well, where n is a positive integer. You can think of this either as scaling up the right triangle by a factor of n, or you can just plug the scaled values into the pythagorean theorem and see that it works.
- Some of the Pythagorean triples we found can be expressed in the form n-$(\frac{n^2-1}{2})$-$(\frac{n^2+1}{2})$, where n is an odd integer greater than 1. This pattern continues.
- Some of the Pythagorean triples we found can be expressed in the form $2n$-(n^2-1)-(n^2+1), where n is an even integer greater than 1. This pattern also continues.

It is not at all necessary to memorize the last two bullet points, but they are quite interesting and may come in handy at times. Knowing a few of these common Pythagorean triples is also quite handy.

There are also some general triangle properties that can be derived from the Pythagorean Theorem.

Proposition 11.6. *For a right triangle $\triangle ABC$ with D being the perpendicular height from B with respect to AC,*

$$DB^2 = (AD)(DC).$$

Proof. For ease of writing, let $AD = x$, $DC = y$, and $DB = z$. From the Pythagorean Theorem, we have

$$\begin{aligned} AB^2 + BC^2 &= AC^2 \\ AB^2 + BC^2 &= (x+y)^2 \\ AB^2 + BC^2 &= x^2 + y^2 + 2 \cdot x \cdot y. \end{aligned}$$

From the Pythagorean Theorem, we also have the following two equations:

$$\begin{aligned} AB^2 &= z^2 + x^2 \\ BC^2 &= z^2 + y^2. \end{aligned}$$

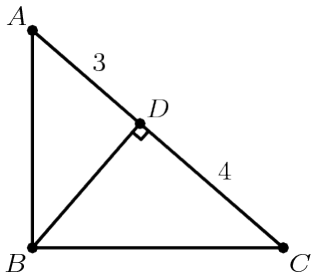
Substituting these into the previous equation,

$$\begin{aligned} z^2 + x^2 + z^2 + y^2 &= x^2 + y^2 + 2 \cdot x \cdot y \\ 2z^2 &= 2xy \\ z^2 &= xy. \end{aligned}$$

Thus, $DB^2 = (AD)(DC)$. ■

Now, let's try a problem that utilizes the previous proposition:

Example 11.7 (2009 AMC10A, modified)**.** Triangle ABC has a right angle at B. Point D is the foot of the altitude from B, $AD = 3$, and $DC = 4$. What is BD?



Solution. Applying the previous proposition, we have

$$\begin{aligned} BD^2 &= (AD)(DC) \\ BD^2 &= 12 \\ BD &= \sqrt{12} \\ BD &= 2\sqrt{3}. \end{aligned}$$

■

§11.3 Area of a Triangle

Now let's investigate the area of a triangle. We'll assume you already know how to find the area of a rectangle (base × height).

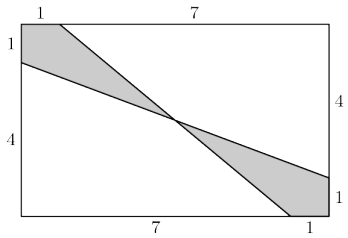
Theorem 11.8 (Area of a Triangle). *A triangle with a base length of length b and a height of length h has area A given by*

$$A = \frac{1}{2}bh.$$

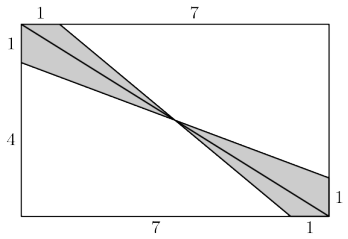
(Remember that height refers to the length of the altitude to the base). Something interesting to note is that there is no unique choice of base and height. Choosing a different base and repeating the calculation with the corresponding height will yield the same result.

These simple area formulas with some creativity are often enough to solve problems. Let's get into some examples!

Example 11.9 (2016 AMC10A). Find the area of the shaded region.



Solution. We can split the shaded regions into triangles as shown in the diagram below:



By symmetry, we can conclude that the height of each triangle is half of the corresponding length or width of the rectangle. Thus,

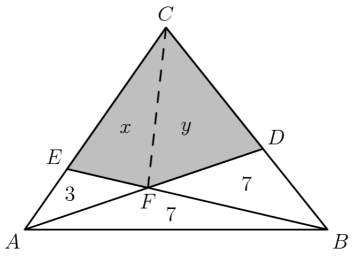
$$\begin{aligned} A &= (2)(\frac{1}{2})(1)(\frac{1+7}{2}) + (2)(\frac{1}{2})(1)(\frac{1+4}{2}) \\ &= 4 + \frac{5}{2} \\ &= \frac{13}{2}. \end{aligned}$$

■

Example 11.10 (Adapted from 2006 AMC 10B). In triangle ABC, cevians AD and BE are drawn, intersecting at point F and creating three smaller triangles and a quadrilateral. Given that the area of $\triangle AEF$ is 3, the area of $\triangle ABF$ is 7, and the area of $\triangle BFD$ is 7,

what is the area of the quadrilateral $CEFD$?

Solution. First, we can divide the quadrilateral in two triangles and label their areas x and y.



Now, compare the areas of triangle that have the same height to compare their bases.

- $\triangle AFB$ and $\triangle FDB$ have the same area. Suppose h_1 is the perpendicular height from point B to line segment AD. Then, by the Area formula

$$\frac{1}{2}(h_1)(AF) = \frac{1}{2}(h_1)(FD)$$
$$AF = FD.$$

- $\triangle AFB$ and $\triangle AEF$ have area 7 and 3, respectively. Suppose h_2 is the perpendicular height from A to EB. Then,

$$\frac{1}{2}(h_2)(EF) = (\frac{3}{7})(\frac{1}{2})(h_2)(FB)$$
$$EF = \frac{3}{7}FB.$$

- Suppose h_3 is the perpendicular height from point C to line segment AD. Because $FD = AF$, we get

$$y = \frac{1}{2}(h_3)(FD)$$
$$y = \frac{1}{2}(h_3)(AF)$$
$$y = x + 3.$$

- Finally, we compare the areas of $\triangle CEF$ and $\triangle CFB$. Suppose h_4 is the perpendicular height from C to EB. Then, the area of $\triangle CEF$ is

$$x = \frac{1}{2}(h_4)(EF).$$

  Finding the area of $\triangle CFB$ and substituting $EF = \frac{3}{7}FB$ in,

$$\begin{aligned} y + 7 &= \frac{1}{2}(h_4)(FB) \\ &= \frac{1}{2}(h_4)(\frac{7}{3})(EF) \\ &= (\frac{7}{3})(\frac{1}{2})(h_4)(EF) \\ &= \frac{7}{3}x. \end{aligned}$$

Now, we have two equations relating the two variables x and y:

$$\begin{cases} y + 7 = \frac{7}{3}x \\ y = x + 3 \end{cases}$$

Using substitution,

$$\begin{aligned} x + 3 + 7 &= \frac{7}{3}x \\ x + 10 &= \frac{7}{3}x \\ 10 &= \frac{4}{3}x \\ x &= \frac{15}{2}. \end{aligned}$$

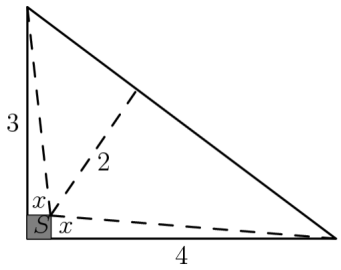
Then, $y = x + 3 = \frac{21}{2}$. This total area of the quadrilateral, which is equivalent to $x + y$, is what we seek. Thus, the answer is $\frac{21}{2} + \frac{15}{2} = 18$. ■

> *Remark.* As seen in the previous example, comparing base lengths between triangles that share a common height is a common theme among elementary area problems.

Now, let's look at some examples that also incorporate the Pythagorean Theorem.

Example 11.11 (2018 AMC 10A). Farmer Pythagoras has a field in the shape of a right triangle. The right triangle's legs have lengths 3 and 4 units. In the corner where those sides meet at a right angle, he leaves a small unplanted square S so that from the air it looks like the right angle symbol. The rest of the field is planted. The shortest distance from S to the hypotenuse is 2 units. What fraction of the field is planted?

Solution. This problem can be solved by splitting the large triangle into a clever set of regions whose areas can be easily computed:



The addition of these lines makes sense because it allows us to utilize the information on the distance from the top-right corner of the square to each side of the triangle.

Computing the area of the large triangle directly, we get

$$A = \frac{1}{2}bh = \frac{1}{2}(3)(4) = 6.$$

Then we compute the area of the large triangle as the sum of multiple regions. The 3 regions include the large triangle with height 2 and hypotenuse as the base, the smaller triangle with

height x and base 4, and the smallest triangle with height x and base 3. Using the Pythagorean Theorem, we find that the hypotenuse is 5. Thus,

$$\begin{aligned} A &= \frac{1}{2}(3)x + \frac{1}{2}(4)(x) + \frac{1}{2}(5)(2) \\ 6 &= \frac{3}{2}x + 2x + 5 \\ 1 &= \frac{7}{2}x \\ \frac{2}{7} &= x. \end{aligned}$$

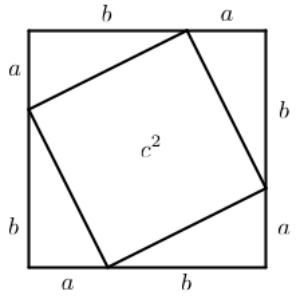
The area of S is $x^2 = \frac{4}{49}$. Then,

$$\frac{\frac{4}{49}}{6} = \frac{2}{147}.$$

of the field is *not* planted. Therefore, the planted portion is $1 - \frac{2}{147} = \frac{145}{147}$.

■

Exercise 11.12. Prove the Pythagorean Theorem (there are many ways to do so).



Hint: One proof utilizes the diagram above and areas.

§11.4 Triangle Similarity and Congruence

Similarity and congruence are concepts we can use to find more information about triangles using what we already know.

If two triangles are **congruent**, then they are identical with respect to the three angles and the three side lengths. Even if one triangle of a congruent pair is rotated or flipped, congruency remains. There are several ways to determine if two triangles are congruent:

1. **Side-Side-Side**: If all three pairs of corresponding sides are equal, then the angles are determined and the triangle is congruent.
2. **Side-Angle-Side**: If two sides and their including angle are the same across two triangles, then the third side is determined and congruency is determined.
3. **Angle-Angle-Side**: If you are given two angles, the third is determined. If any side is the same as in another triangle, then congruency is determined.
4. **Hypotenuse-Leg**: If both of these sides are known to be of same length of corresponding parts of other right triangles, then the third leg is determined and congruence is proven.

Often, congruence is not found on its own in geometry problems. Instead, you will see it coupled with the concept of similarity.

If two triangles are **similar**, then their angles are identical. They must be the same shape, but not necessarily the same size. Here are some ways to determine similarity:

1. **Side-Side-Side**: If ratios of all three pairs of corresponding sides are all equal, then the triangles are similar. However, this is not very common to spot.
2. **Side-Angle-Side**: If the corresponding angles are the same and both pairs of its neighboring sides are proportional with the same ratio, then the triangles are similar.
3. **Angle-Angle**: This is the most common indicator. If two corresponding pairs of angles are the same, the third angle should also be the same, thus determining similarity.
4. **Hypotenuse-Leg**: This only applies to right triangles. If the ratio of hypotenuse to one leg is the same, then the other leg is determined for both triangles and the angles are determined as well.

Theorem 11.13. *If two triangles ABC and DEF are similar $ABC \sim DEF$ (in that specific order of angles), then*

$$\angle A = \angle D, \angle B = \angle E, \angle C = \angle F$$

and

$$\frac{AB}{DE} = \frac{BC}{EF} = \frac{AC}{DF} = k.$$

*We call k the **scale factor**.*

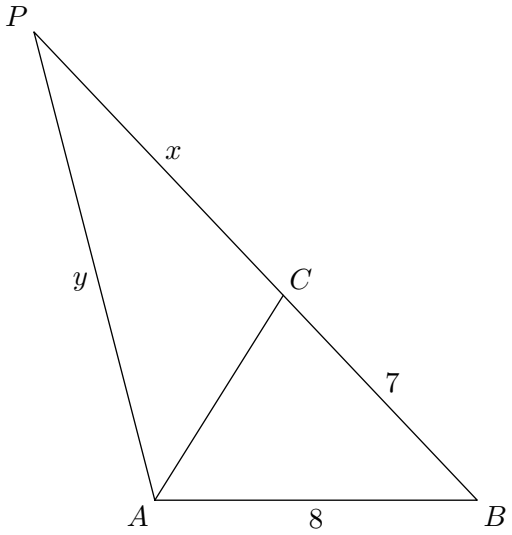
Remark. This property isn't confined to sides either. For example, if triangle ABC has circumradius R and triangles ABC and DEF are similar with scale factor k, then triangle DEF has circumradius $\frac{R}{k}$. Or, if the distance between A and the orthocenter of triangle ABC is x, then the distance between D and the orthocenter of triangle DEF is $\frac{x}{k}$.

For area, the scale factor is squared: if the area of triangle ABC is S, then the area of triangle DEF is $\frac{S}{k^2}$. You can prove this using our area formulas.

We will demonstrate the similarity principle below:

Example 11.14 (Adapted from AHSME 1986)**.** In $\triangle ABC$, $AB = 8$, $BC = 7$, $CA = 6$ and side BC is extended to a point P so that $\triangle PAB$ is similar to $\triangle PCA$. What is the length of PC?

Solution. As always, draw a diagram and assign variables to unknown lengths:



Since we are given that $\triangle PAB \sim \triangle PCA$, we can form the following proportions and conclusions:

$$\frac{PA}{AB} = \frac{PC}{CA} \implies \frac{y}{8} = \frac{x}{6} \implies 4x = 3y$$

$$\frac{PB}{AB} = \frac{PA}{CA} \implies \frac{x+7}{8} = \frac{y}{6} \implies 8y = 6x + 42$$

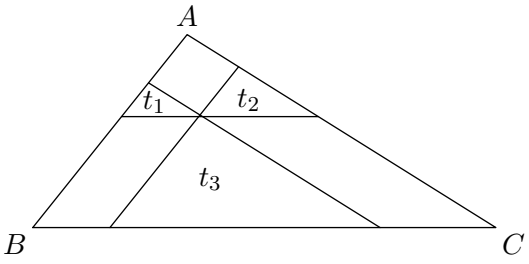
At this point, we have two equations and two unknown variables, which we know how to solve! We get that $PC = x = 9$, and this is our answer.

■

Now we'll move on to a problem that gives insight about areas.

Example 11.15 (Adapted from 1984 AIME). A point P is chosen in the interior of $\triangle ABC$ such that when lines are drawn through P parallel to the sides of $\triangle ABC$, the resulting smaller triangles t_1, t_2, and t_3 formed by the lines have areas 4, 9, and 49, respectively. Find the area of $\triangle ABC$.

Solution. As always with geometry problems, draw a diagram.



These smaller triangles are similar to each other and to $\triangle ABC$ due to angle similarity. Convince yourself why this is true.

Looking back at the remark regarding similarity, we see that by taking the square root of each of these areas, we get their relative side length proportions: $2, 3$, and 7. Now, take the bottom side of each smaller triangle and call them $2x, 3x$, and $7x$. This means that $BC = 12x$. This is because the existence of parallelograms in the figure means that opposite sides are congruent. Make sure you agree with this line of reasoning. Now, we get that the side length proportions

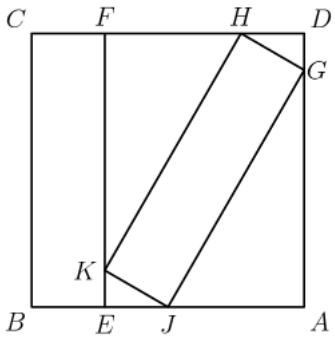
(including $\triangle ABC$ at the end) are $2:3:7:12$. Square each of these to get back to area proportions, and we get that the area of $\triangle ABC = 144$.

■

Now for a trickier one. The following problem also highlights an important strategy: If you can't see many congruent/similar triangles in a diagram, draw some lines and make some up!

Example 11.16 (2014 AMC 12B). Let $ABCD$ be a square of side length 1. Points E and F lie on AB and CD respectively such that $CFEB$ is a rectangle. Points K, H, G, and J lie on EF, FD, DA, and AE respectively such that the rectangles $JKHG$ and $EBCF$ are congruent. What is BE?

Solution. First things first: draw a diagram. Call $BE = x$. Now we should draw some lines.



Specifically, we can draw a line from H that intersects AB at a right angle. Call this point L. Now, draw line HJ. Note that

$$\triangle HKJ \cong \triangle HLJ$$

because of the Hypotenuse-Leg congruence theorem and

$$\triangle KEJ \cong \triangle GDH$$

via the ASA congruence theorem. (Can you figure out why?) Now, since corresponding parts of congruent triangles are congruent, $JL = 1$. Now,

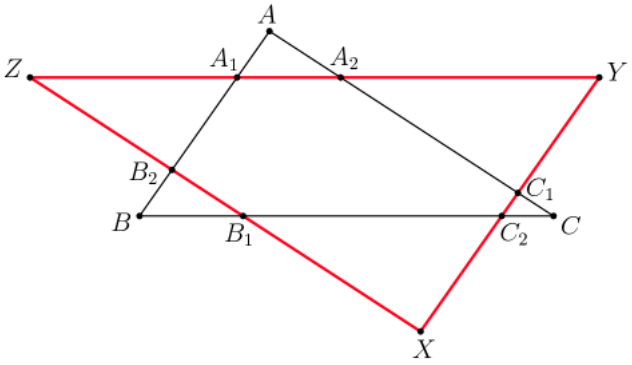
$$BE = JL, EJ = HD = LA \implies BE + EJ = JL + LA \implies BJ = JA \implies BJ = JA = \frac{1}{2}$$

Since we know that $GJ = 1$ and $JA = \frac{1}{2}$, $GA = \frac{\sqrt{3}}{2}$ because of the Pythagorean Theorem. Thus, $KE = DG = \frac{2-\sqrt{3}}{2}$. Now, focusing on right triangle KEJ, we can solve for x using the Pythagorean Theorem:

$$(KE)^2 + (EJ)^2 = (KJ)^2 \implies \left(\frac{2-\sqrt{3}}{2}\right)^2 + \left(\frac{1}{2} - x\right)^2 = x^2.$$

Through some algebra, we get that $x = 2 - \sqrt{3}$. ■

Example 11.17 (2019 AIME II)**.** Triangle ABC has side lengths $AB = 120$, $BC = 220$, and $AC = 180$. Lines ℓ_A, ℓ_B, and ℓ_C are drawn parallel to $\overline{BC}$, $\overline{AC}$, and $\overline{AB}$, respectively, such that the intersection of ℓ_A, ℓ_B, and ℓ_C with the interior of $\triangle ABC$ are segments of length 55, 45, and 15, respectively. Find the perimeter of the triangle whose sides lie on ℓ_A, ℓ_B, and ℓ_C.



Solution. Label points as in the diagram on the next page. Note that triangle AA_1A_2 is similar to triangle ABC. Thus,

$$\frac{AB}{AA_1} = \frac{BC}{A_1A_2} = \frac{AC}{AA_2} \implies \frac{120}{AA_1} = \frac{220}{55} = \frac{180}{AA_2}.$$

This means that $AA_1 = 30$ and $AA_2 = 45$. By the same reasoning, we find $BB_1 = 55$, $BB_2 = 30$, $CC_1 = 22.5$, and $CC_2 = 27.5$ — make sure to confirm for yourself that this works! Now, by subtracting lengths, we get that $A_1B_2 = 60$, $B_1C_2 = 137.5$, and $C_1A_2 = 112.5$.

But there are more similar triangles to work with — one example being triangles AA_1A_2 and B_2A_1Z. Pause for a moment and see if you can find the others.

Because of this, we have $\frac{ZB_2}{AA_2} = \frac{ZA_1}{A_1A_2} = \frac{A_1B_2}{A_1A}$, from which we find $ZA_1 = 110$ and $ZB_2 = 90$. From the other similar triangle pairs, we deduce that $YA_2 = 137.5$, $YC_1 = 75$, $XB_1 = 112.5$, and $XC_2 = 75$. We now have all of the lengths to complete the problem!

Our answer is

$$\begin{aligned} XY + YZ + ZX &= ZA_1 + A_1A_2 + A_2Y + YC_1 + C_1C_2 + C_2X + XB_1 + B_1B_2 + B_2Z \\ &= 110 + 55 + 137.5 + 75 + 15 + 75 + 112.5 + 45 + 90 \\ &= 715 \end{aligned}$$

and we are done. ■

§11.5 Homework Problems

Problem 11.1 (Adapted from 2011 AMC 8)**.** [3] Let A be the area of the triangle with sides of length $25, 25$, and 30. Let B be the area of the triangle with sides of length $25, 25$, and 40. What is $\dfrac{A}{B}$?

Problem 11.2 (Adapted from 2002 AMC 10B)**.** [5] A regular octagon $ABCDEFGH$ has sides of length two. The area of $\triangle ADG$ can be expressed in the form $a + b\sqrt{c}$ The square of the area of the triangle with sides a, b, and c can be expressed ad d (which can be 0 if the triangle is impossible or degenerate). Find $10000d$.

Problem 11.3 (2018 AMC 8)**.** [4] In $\triangle ABC$, a point E is on $\overline{AB}$ with $AE = 1$ and $EB = 2$. Point D is on $\overline{AC}$ so that $\overline{DE} \parallel \overline{BC}$ and point F is on $\overline{BC}$ so that $\overline{EF} \parallel \overline{AC}$. The ratio of the area of $CDEF$ to the area of $\triangle ABC$? can be expressed as $\frac{a}{b}$. Find $a + b$.

Problem 11.4 (2017 CMIMC)**.** [3] Let ABC be a triangle with $\angle BAC = 117°$. The angle bisector of $\angle ABC$ intersects side AC at D. Suppose $\triangle ABD \sim \triangle ACB$. Compute the measure of $\angle ABC$, in degrees.

Problem 11.5 (2000 AMC 12)**.** [5] Through a point on the hypotenuse of a right triangle, lines are drawn parallel to the legs of the triangle so that the triangle is divided into a square and two smaller right triangles. The area of one of the two small right triangles is m times the area of the square. If the ratio of the area of the square to the area of the other small right triangle can be expressed as am where a is an integer, what is a?

Problem 11.6 (2007 AMC 10B)**.** [5] Right $\triangle ABC$ has $AB = 3, BC = 4$, and $AC = 5$. Square $XYZW$ is inscribed in $\triangle ABC$ with X and Y on $\overline{AC}, W$ on $\overline{AB}$, and Z on $\overline{BC}$. If the side length of the square can be expressed as the common fraction $\frac{m}{n}$, what is $m + n$?

Problem 11.7 (2017 AMC 10B)**.** [6] The diameter $\overline{AB}$ of a circle of radius 2 is extended to a point D outside the circle so that $BD = 3$. Point E is chosen so that $ED = 5$ and the line ED is perpendicular to the line AD. Segment $\overline{AE}$ intersects the circle at point C between A and E. If the area of $\triangle ABC$ can be expressed as $\frac{a}{b}$, where a and b are positive integers, what is $a + b$?

Problem 11.8 (Adapted from 2017 AMC 10A)**.** [6] A square with side length x is inscribed in a right triangle with sides of length 3, 4, and 5 so that one vertex of the square coincides with the right-angle vertex of the triangle. A square with side length y is inscribed so that one side of the square lies on the hypotenuse of the triangle. The ratio $\frac{x}{y}$, when simplified, gets the common fraction $\frac{a}{b}$. What is $a^2 - b^2$?

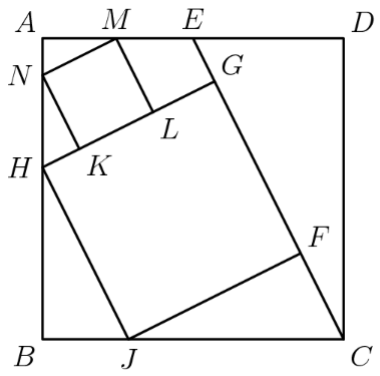
Problem 11.9 (2020 AMC 10B)**.** [6] In square $ABCD$, points E and H lie on $\overline{AB}$ and $\overline{DA}$, respectively, so that $AE = AH$. Points F and G lie on $\overline{BC}$ and $\overline{CD}$, respectively, and points I and J lie on $\overline{EH}$ so that $\overline{FI} \perp \overline{EH}$ and $\overline{GJ} \perp \overline{EH}$. Triangle AEH, quadrilateral $BFIE$, quadrilateral $DHJG$, and pentagon $FCGJI$ each has area 1. FI^2 can be expressed in the form $a - b\sqrt{c}$. What is $a + b + c$?

Problem 11.10 (2006 AIME II)**.** [7] Square $ABCD$ has sides of length 1. Points E and F are on $\overline{BC}$ and $\overline{CD}$, respectively, so that $\triangle AEF$ is equilateral. A square with vertex B has sides that are parallel to those of $ABCD$ and a vertex on $\overline{AE}$. The length of a side of this smaller square is $\frac{a-\sqrt{b}}{c}$, where a, b, and c are positive integers and b is not divisible by the square of any prime. Find $a + b + c$.

Problem 11.11 (2018 AIME I)**.** [8] In $\triangle ABC, AB = AC = 10$ and $BC = 12$. Point D lies strictly between A and B on $\overline{AB}$ and point E lies strictly between A and C on $\overline{AC}$ so that $AD = DE = EC$. Then AD can be expressed in the form $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p + q$.

Problem 11.12 (2015 AIME I)**.** [7]

$ABCD$ is a square. Point E is the midpoint of $\overline{AD}$. Points F and G lie on $\overline{CE}$, and H and J lie on $\overline{AB}$ and $\overline{BC}$, respectively, so that $FGHJ$ is a square. Points K and L lie on $\overline{GH}$, and M and N lie on $\overline{AD}$ and $\overline{AB}$, respectively, so that $KLMN$ is a square. The area of $KLMN$ is 99. Find the area of $FGHJ$.



Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

12 Circles

In this handout, we'll go over many important topics related to circles.

§12.1 Arcs

Proposition 12.1 (Prerequisites). *Given a circle with radius r and a point A outside the circle,*

- *The area of the circle is πr^2.*
- *The circumference of a circle is $2\pi r$.*
- *A line passing through A that is tangent to the circle is perpendicular to the radius passing through the point of tangency.*

For the sake of simplicity, we will now include most of the properties of arcs below. These properties are fairly simple, but they can be used to prove many stronger statements.

Proposition 12.2 (Properties of Arcs). *Let $\overset{\frown}{XY}$ denote the length of arc XY. Given a circle with center O, radius r, and four points A, B, C, D on this circle,*

- ***(Inscribed Angle Theorem)*** *$\angle ABC = \frac{1}{2}\angle AOC$.*
- *$AB = CD$ if and only if $\overset{\frown}{AB} = \overset{\frown}{CD}$.*
- *Given that θ is $\angle AOB$ measured in radians and θ_0 is $\angle AOB$ measured in degrees,*

$$\overset{\frown}{AB} = r\theta = 2\pi r\frac{\theta_0}{360}$$

In other words, in a circle, the length of an arc is proportional to the central angle.

Now that we know have this information, we are ready to tackle some problems! Make sure you understand what the statements above are saying, because that will really help with solving problems about arcs and arc lengths!

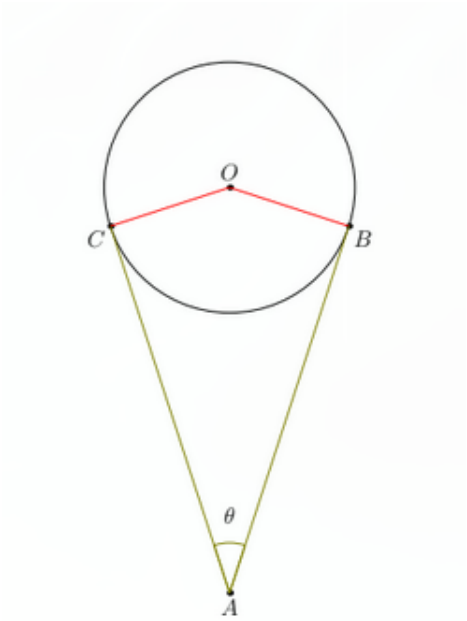
Example 12.3 (2011 AMC 12B). Two tangents to a circle are drawn from a point A. The points of contact B and C divide the circle into arcs with lengths in the ratio $2 : 3$. What is the degree measure of $\angle BAC$?

Solution. The first thing we do is draw a diagram and label the important points.

Let the center of the circle be O. Then, we see that the question is asking for an angle when we are only given the length of an arc. This is where Part 3 of Proposition 12.2 comes in.

However, we can't use that directly, as we need to simplify the expression first. We know that $\angle BOC = 2\theta$ for some θ. We also know $2\theta + 3\theta = 360^\circ \implies \theta = 72^\circ$. This means that $\angle BOC = 144^\circ$.

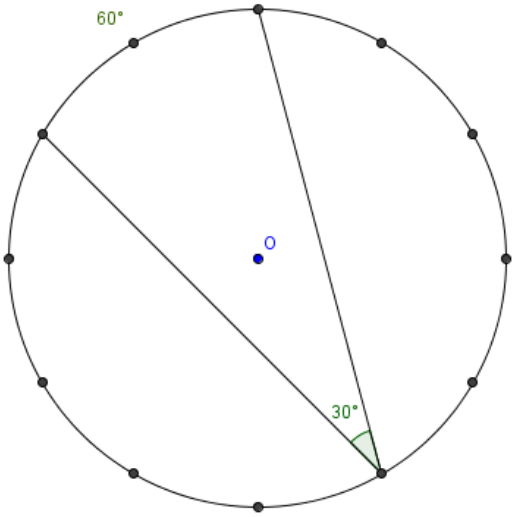
We know what $\angle BOC$ is now, but we want to relate that to $\angle BAC$. How do we do that? If we look at the diagram for some time, we see that



$ABOC$ is a quadrilateral, so $\angle ABO + \angle BOC + \angle OCA + \angle CAB = 360^\circ \implies 90^\circ + 144^\circ + 90^\circ + \angle CAB = 360^\circ \implies \angle CAB = \angle BAC = 36^\circ$. ■

Example 12.4 (2007 AMC 12A)**.** A star-polygon is drawn on a clock face by drawing a chord from each number to the fifth number counted clockwise from that number. That is, chords are drawn from 12 to 5, from 5 to 10, from 10 to 3, and so on, ending back at 12. What is the degree measure of the angle at each vertex in the star polygon?

Solution. Once again, we start with drawing a diagram.



It should be obvious that every angle is the same, so let's look at the angle between 1, 6, and 11. Call the point at 1 A, the point at 6 B, the point at 11 C, and the center of the clock O. We want to calculate the angle of an inscribed angle, so the Inscribed Angle Theorem. However, we can't use that just yet, as we need to simplify first.

We know that $\overset{\frown}{AC}$ is $\frac{1}{6}$ of the circumference of the clock (see diagram!), so $\angle AOC = \frac{1}{6} \cdot 360° = 60°$. By the Inscribed Angle Theorem, $\angle ABC = \frac{1}{2}\angle AOC = \frac{1}{2} \cdot 60° = 30°$. ■

Example 12.5 (2002 AMC 12A). A 45° arc of circle A is equal in length to a 30° arc of circle B. What is the ratio of circle A's area and circle B's area?

Solution. As always, we label points first. Let r_A be the radius of circle A and let r_B be the radius of circle B. Once again, we want to relate the central angle to the length of an arc, so we will probably use Part 3 of Proposition 12.2.

$$2\pi r_A \cdot \frac{45}{360} = 2\pi r_B \cdot \frac{30}{360} \implies r_A \cdot \frac{1}{8} = r_B \cdot \frac{1}{12} \implies r_B = \frac{3}{2} \cdot r_A.$$

The ratio of A's area to B's area is

$$\frac{\pi r_A^2}{\pi(\frac{3r_A}{2})^2},$$

which is $(\frac{2}{3})^2 = \frac{4}{9}$. Make sure you don't misread the question and forget to square $\frac{2}{3}$! ■

Arcs may seem a bit intimidating at first, but they're really not that bad. Once you get used to them and are used to using Proposition 12.2, they should become a piece of cake!

Exercise 12.6. Prove all parts of Proposition 12.2.

§12.2 Cyclic Quadrilaterals

Definition 12.7. A **cyclic quadrilateral** is a quadrilateral that can be inscribed in a circle.

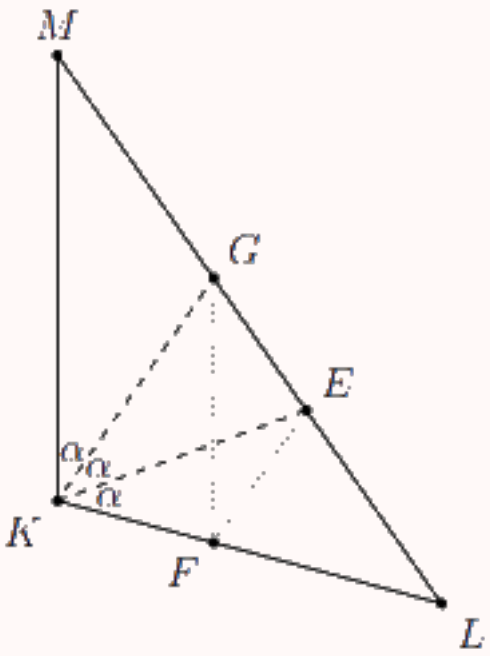
Theorem 12.8 (Cyclic Quadrilaterals). *Given a convex quadrilateral $ABCD$, the following statements are all equivalent:*

1. *$ABCD$ is cyclic.*
2. *$\angle ABD = \angle ACD$.*
3. *$\angle ABC + \angle CDA = 180°$.*

This theorem may seem insignificant, but it can be applied in many different ways. This is arguably *the* most important theorem when trying to angle chase. In most cases, the problem may not seem to have a cyclic quadrilateral, but if you look hard enough (don't literally stare at a piece of paper!), oftentimes you will find one that will help you solve a problem.

Exercise 12.9. Prove that a trapezoid is cyclic if and only if it is isosceles.

Example 12.10 (COMC 2019). In triangle KLM, let points G and E be on segment LM so that $\angle MKG = \angle GKE = \angle EKL = \alpha$. Let point F be on segment KL so that GF is parallel to KM. Given that $KFEG$ is an isosceles trapezoid and that $\angle KLM = 84°$, determine α.



Solution. When we are trying to find angles, the first thing we should do is try to find cyclic quadrilaterals. We are given that $KFEG$ is an isosceles trapezoid, so it is also cyclic. This means that $\angle FGE = \angle FKE = \alpha$ (By Part 2 of Theorem 12.8). It may seem like we are stuck, until we read the question again and realize that we are given that GF is parallel to KM, so $\angle GFL = \angle KML = 3\alpha$.
We also know that the sum of the three angles of $\triangle GFL$ is $180°$, so $3\alpha + \alpha + 84° = 180° \implies 4\alpha = 96° \implies \alpha = 24°$. ■

This problem taught us that if we are stuck at some point in a problem, it's never a bad idea to read the problem statement again and see what condition we haven't used yet.
While Theorem 12.8 is very powerful, when solving computational problems, it is often not enough. Here is another useful theorem that will make solving problems much easier.

Theorem 12.11 (Ptolemy's Theorem). *Given any four points,*

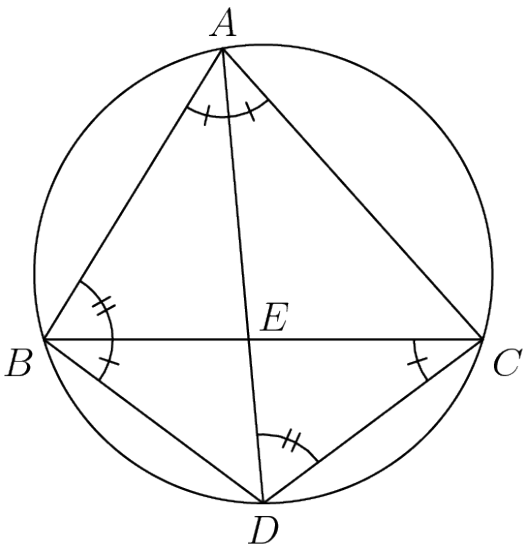
$$AB \cdot CD + BC \cdot DA \geq AC \cdot BD,$$

where equality holds if and only if $ABCD$ is a cyclic quadrilateral.

This theorem can seem intimidating at first, but it is very useful and worth remembering.

Example 12.12 (2004 AMC 10B). In triangle ABC we have $AB = 7$, $AC = 8$, $BC = 9$. Point D is on the circumscribed circle of the triangle so that AD bisects angle BAC. What is the value of $\frac{AD}{CD}$?

Solution. Let $CD = a$ and $AD = b$ (labelling the points!).



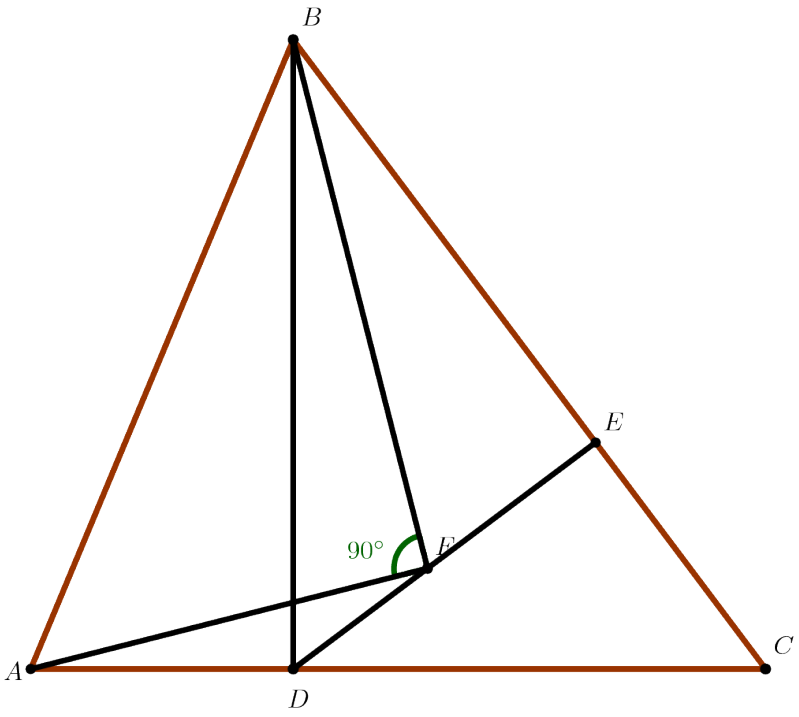
We know that we want to use Ptolemy's because the question deals with lengths, not just angles. AD bisects $\angle BAC$, so $\angle BAD = \angle DAC \implies \widehat{BD} = \widehat{DC} \implies BD = a$. By Ptolemy's Theorem,

$$AB \cdot CD + AC \cdot BD = AD \cdot BC \implies 7a + 8a = 9b \implies 15a = 9b.$$

To find $\frac{AD}{CD} = \frac{b}{a}$ we simply multiply both sides of the equation by $\frac{1}{9a}$ to get $\frac{15}{9} = \frac{5}{3}$. ■

Of course, there are many other solutions, and you don't have to Ptolemy's Theorem. In fact, try finding a solution that does not involve Ptolemy's!

Example 12.13 (2013 AMC 12B)**.** In triangle ABC, $AB = 13$, $BC = 14$, and $CA = 15$. Distinct points D, E, and F lie on segments $\overline{BC}$, $\overline{CA}$, and $\overline{DE}$, respectively, such that $\overline{AD} \perp \overline{BC}$, $\overline{DE} \perp \overline{AC}$, and $\overline{AF} \perp \overline{BF}$. The length of segment $\overline{DF}$ can be written as $\frac{m}{n}$, where m and n are relatively prime positive integers. What is $m + n$?



Solution. We first solve for AD, because it is fairly easy to find and it may make the problem much simpler. Using Heron's Formula, we know that the area of $\triangle ABC$ is

$$\frac{1}{2} \cdot 14 \cdot AD = \sqrt{(21)(6)(7)(8)} = 84,$$

so $AD = 12$.

We can look at the diagram and try to find cyclic quadrilaterals. After eyeballing some quadrilaterals and trying to prove whether or not they are cyclic, we find that $AFDB$ is cyclic because $\angle AFB = \angle ADB = 90°$, so $\angle ABF = \angle ADF \implies \triangle ABF \sim \triangle ADE \sim \triangle ACD$ (by AA).

By the Pythagorean Theorem, $DC = 9$, so

$$\frac{AB}{BF} = \frac{AC}{CD} \implies \frac{13}{BF} = \frac{15}{9} \implies BF = \frac{13 \cdot 3}{5}.$$

Similarly,

$$\frac{AB}{AF} = \frac{AC}{AD} \implies \frac{13}{AF} = \frac{15}{12} \implies AF = \frac{13 \cdot 4}{5}.$$

Now, we see that we have almost every side of the cyclic quadrilateral (other than DE, the side we want). This is a sign that Ptolemy's Theorem may come in handy. By Ptolemy's,

$$AB \cdot DF + AF \cdot BD = AD \cdot BF \implies 13 \cdot DF + \frac{13 \cdot 4}{5} \cdot (14 - 9) = 12 \cdot \frac{13 \cdot 3}{5}.$$

When we divide both sides by 13, we get

$$DF + 4 = \frac{36}{5} \implies DF = \frac{16}{5}.$$

We are asked to find $m + n = 16 + 5 = 21$. ■

This problem looks intimidating at first, but it's not too bad once you have some lengths down.

In the future, if there is a problem with a bunch of unknowns and you're stuck, it's not a bad idea to try and find some random lengths and see where that gets you (of course, only do this is the lengths are really easy to find!). Cyclic quadrilaterals are something one needs to take a while to get used to, but once you are familiar with them they can be very helpful!

Exercise 12.14. Two different points, C and D, lie on the same side of line AB so that $\triangle ABC$ and $\triangle BAD$ are congruent with $AB = 9$, $BC = AD = 10$, and $CA = DB = 17$. The intersection of these two triangular regions has area $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

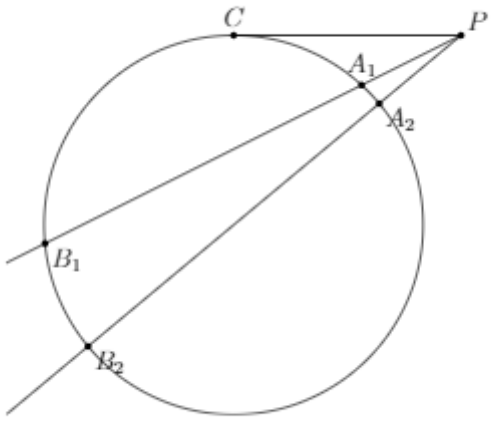
§12.3 Power of a Point

Theorem 12.15 (Power of a Point). *This theorem has two parts.*

- *Fix two chords AB, CD of a circle. Let them intersect at a point P inside the circle. Then $PA \cdot PB = PC \cdot PD$.*
- *Fix two lines r, s and a circle ω, none of which are parallel to each other. r and s pass through a point P outside of the circle.*

  Let r intersect ω at A_1 and B_1 and s intersect ω at A_2 and B_2. Then $PA_1 \cdot PB_1 = PA_2 \cdot PB_2$.

*We let the **power** of each point be the product in both parts of this theorem. The power of points on the circle is 0.*



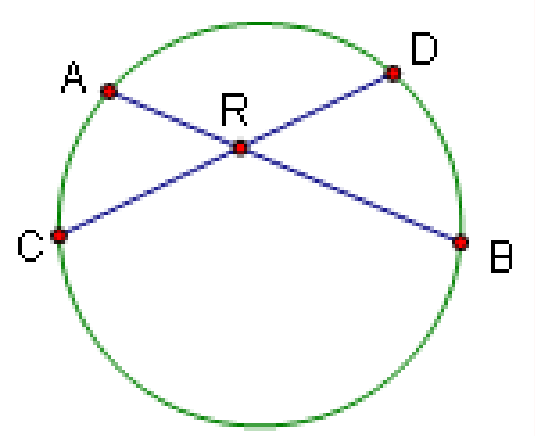
Proof. We prove each part of the theorem separately.

- We claim that $\triangle PAC \sim \triangle PBD$. Note that $\angle APC = \angle BPD$ because of vertical angles, and $\angle CAP = \angle BDP$ and $\angle ACP = \angle DBP$ from inscribed angles. Therefore, $\triangle PAC \sim \triangle PDB$, and it follows that $PA/PC = PD/PB \implies PA \cdot PB = PC \cdot PD$.
- We claim that $\triangle PA_1A_2 \sim \triangle PB_2B_1$. Note that $\angle PA_1A_2 = 180^\circ - \angle B_1A_1A_2 = \angle PB_2B_1$. It's quite obvious that $\angle A_1PA_2 = \angle B_1PB_2$ as well, so by AA similarity we have that $\triangle PA_1A_2 \sim \triangle PB_2B_1$. Our length ratios follow immediately.

■

Note. If the circle is tangent, we sometimes say that it intersects the same point twice. Therefore, it follows that if a line from P is tangent to the circle at C, then the power of P is PC^2.

Example 12.16 (ARML). In a circle, chords AB and CD intersect at R. If $AR : BR = 1 : 4$ and $CR : DR = 4 : 9$, find the ratio $AB : CD$.



Solution. Let $AR = x, BR = y$. We then have that $AB = 5x, CD = 13y$. It suffices to find $\dfrac{5x}{13y}$, which is equivalent to $\left(\dfrac{5}{13}\right)\left(\dfrac{x}{y}\right)$. From Power of a Point, we have that $x \cdot 4x = 4y \cdot 9y$,

so it follows that

$$\begin{aligned} 4x^2 &= 36y^2 \\ \implies \left(\frac{x}{y}\right)^2 &= 9 \\ \implies \frac{x}{y} &= 3. \end{aligned}$$

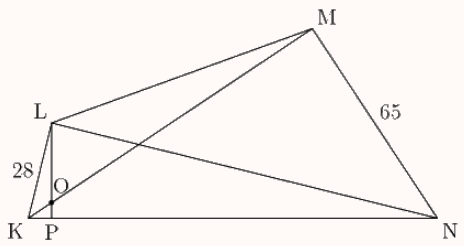
Hence, the desired ratio is $\frac{5}{13} \cdot 3 = \frac{15}{13}$. ■

Example 12.17 (2013 AMC 10A)**.** In $\triangle ABC$, $AB = 86$, and $AC = 97$. A circle with center A and radius AB intersects $\overline{BC}$ at points B and X. Moreover $\overline{BX}$ and $\overline{CX}$ have integer lengths. What is BC?

Solution. Let our circle meet line AC at points Y, Z, such that Y is closer to C. It follows that $AY = AZ = 86$. Therefore, $CY = 97 - 86 = 11$ and $CZ = 11 + 86 \cdot 2 = 183$. Hence, from Power of a Point, $BC \cdot CX = 11 \cdot 183$.

As BX and CX must be integral, so must BC. Therefore, we need two integers a, b such that $a > b$ and $ab = 3 \cdot 11 \cdot 61$. Because a is equal to BC, we must also have $a + 86 > 97$ and that $a < 86 + 97 = 183$. Trying all solution pairs, it can be found that $a = 61$ is the only valid solution. ■

Example 12.18 (2019 AIME I)**.** In convex quadrilateral $KLMN$ side $\overline{MN}$ is perpendicular to diagonal $\overline{KM}$, side $\overline{KL}$ is perpendicular to diagonal $\overline{LN}$, $MN = 65$, and $KL = 28$. The line through L perpendicular to side $\overline{KN}$ intersects diagonal $\overline{KM}$ at O with $KO = 8$. Find MO.



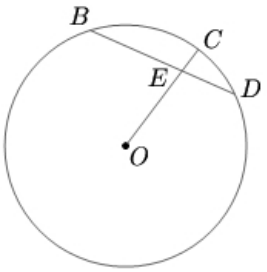
Solution. Let the foot of the altitude from L to KN be P. Note that $NPOM$ is cyclic because $\angle OPN = \angle OMN = 90°$. Also note that (NPL) is tangent to KL. Hence, we have that $KO \cdot KM = 8 \cdot KM = KP \cdot KN = KL^2 = 28^2$. Hence, $KM = \frac{28^2}{8} = 98$, so $MO = 98 - 8 = 90$. ■

§12.4 Homework Problems

Problem 12.1 (2007 AMC 10B)**.** [3] The point O is the center of the circle circumscribed about $\triangle ABC$, with $\angle BOC = 120°$ and $\angle AOB = 140°$, as shown. What is the degree measure of $\angle ABC$?

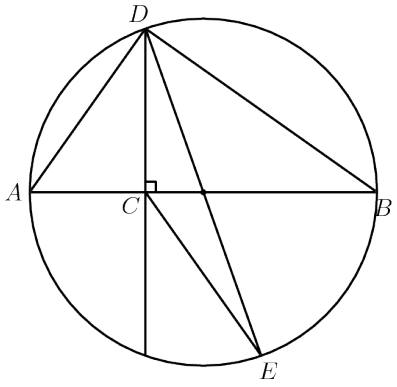
Problem 12.2 (2020 AMC 12B)**.** [4] In unit square $ABCD$, the inscribed circle ω intersects $\overline{CD}$ at M, and $\overline{AM}$ intersects ω at a point P different from M. Given that $AP = \frac{\sqrt{a}}{b}$, where this fraction is simplified, what is $a + b$?

Problem 12.3 (1971 Canada)**.** [4] DEB is a chord of a circle such that $DE = 3$ and $EB = 5$. Let O be the center of the circle. Join OE and extend OE to cut the circle at C. Given $EC = 1$, find the radius of the circle.



Problem 12.4 (2020 AMC 12B)**.** [6] Let $\overline{AB}$ be a diameter in a circle of radius $5\sqrt{2}$. Let $\overline{CD}$ be a chord in the circle that intersects $\overline{AB}$ at a point E such that $BE = 2\sqrt{5}$ and $\angle AEC = 45^\circ$. What is $CE^2 + DE^2$?

Problem 12.5 (2005 AMC 12A)**.** [6] Let $\overline{AB}$ be a diameter of a circle and C be a point on $\overline{AB}$ with $2 \cdot AC = BC$. Let D and E be points on the circle such that $\overline{DC} \perp \overline{AB}$ and $\overline{DE}$ is a second diameter. If the ratio of the area of $\triangle DCE$ to the area of $\triangle ABD$ is $\frac{a}{b}$, where this fraction is simplified, what is $a + b$?



Problem 12.6 (2005 AIME I)**.** [6]

Triangle ABC has $BC = 20$. The incircle of the triangle evenly trisects the median AD. If the area of the triangle is $m\sqrt{n}$ where m and n are integers and n is not divisible by the square of a prime, find $m + n$.

Problem 12.7 (2017 AMC12B)**.** [7] The diameter AB of a circle of radius 2 is extended to a point D outside the circle so that $BD = 3$. Point E is chosen so that $ED = 5$ and line ED is perpendicular to line AD. Segment AE intersects the circle at a point C between A and E. Given that the area of $\triangle ABC$ is $\frac{a}{b}$, where this fraction is simplified, what is $a + b$?

Problem 12.8 (2014 AMC 12B)**.** [10] Let $ABCDE$ be a pentagon inscribed in a circle such that $AB = CD = 3$, $BC = DE = 10$, and $AE = 14$. The sum of the lengths of all diagonals of $ABCDE$ is equal to $\frac{m}{n}$, where m and n are relatively prime positive integers. What is $m + n$?

Problem 12.9 (2008 iTest)**.** [8] Points C and D lie on opposite sides of line $\overline{AB}$. Let M and N be the centroids of $\triangle ABC$ and $\triangle ABD$ respectively. If $AB = 841$, $BC = 840$, $AC = 41$, $AD = 609$, and $BD = 580$, find the sum of the numerator and denominator of the value of MN when expressed as a fraction in lowest terms.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

13 Triangles II

In this handout, we'll build on our knowledge of triangles and tackle some more advanced concepts.

§13.1 Triangle Centers

In this section, we describe the properties of the most common triangle centers, i.e. special points associated with each triangle. The proofs are just as important to understand as the properties themselves, and provide useful intuition, so we strongly urge you try to do every exercise in the section.

As usual, and especially with geometry, its important to have pencil and paper handy. It's almost impossible (or at least very ineffective) to go through examples without drawing the diagrams yourself to follow along.

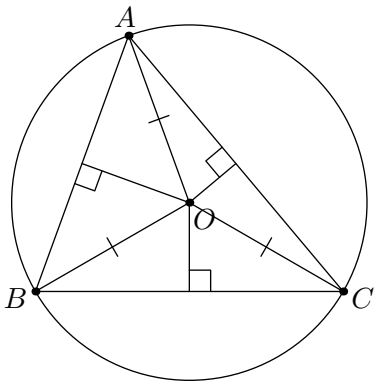
§13.1.1 Circumcenter

Definition 13.1. The **perpendicular bisector** of a segment AB is the locus (i.e. collection) of points C such that $AB = AC$.

Exercise 13.2. Show that the perpendicular bisector of a segment AB is the line perpendicular to AB passing through its midpoint.

Hint: Why does the midpoint M always lie on the perpendicular bisector? Then show that any other point on the perpendicular bisector lies on the line perpendicular to AB and passing through M using congruent triangles.

Theorem 13.3 (Circumcenter). *In any triangle $\triangle ABC$, the perpendicular bisectors of its sides concur at a point O, the **circumcenter** of the triangle.*



Exercise 13.4. Prove that the perpendicular bisectors concur at a point O.

Hint: Let two perpendicular bisectors meet at O, and then show that the third one must pass through O as well.

Exercise 13.5. Show that there exists a circle with center at O passing through A, B, and C, $\triangle ABC$'s **circumcircle**.

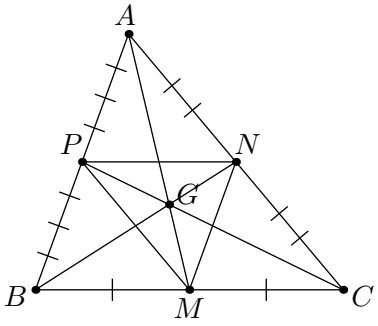
Hint: The radius of the circle should be AO. Why must this length also be the distance from O to B and O to C?

Exercise 13.6. Show that this implies that three points uniquely define a circle; that is, show that there exists exactly one circle passing through any three given points.

Hint: Use a proof by contradiction. A circle is different from another circle if and only if they either have different centers, radii, or both, so assume that there exists two circles passing through some points A, B, and C, and show that they must be the same.

§13.1.2 Centroid

Definition 13.7. The **median** from a vertex A of a triangle $\triangle ABC$ is the line from A to the midpoint of $\overline{BC}$.



Definition 13.8. The **medial triangle** of a triangle $\triangle ABC$ is the triangle formed by the midpoints of its sides.

Proposition 13.9. *In a triangle $\triangle ABC$, if the midpoints of BC, CA, and AB are M, N, and P, respectively, then $\triangle MNP \cong \triangle ANP \cong \triangle BPM \cong \triangle CMN$, and all four triangles are similar to $\triangle ABC$.*

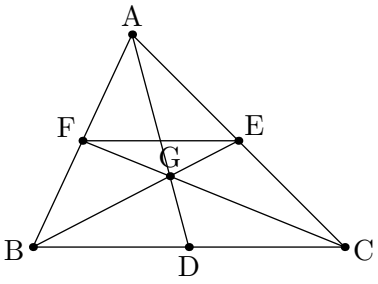
Exercise 13.10. Prove that $\triangle MNP \cong \triangle ANP$.

Exercise 13.11. Prove that $\triangle MNP \sim \triangle ABC$.

Theorem 13.12 (Centroid)**.** *In a triangle $\triangle ABC$, the medians of the triangle meet at a point G, the **centroid** of the triangle.*

Proof. Let BE intersect CF at G. Since $\triangle AFE \sim \triangle ABC$, $FE \parallel BC$. Thus $\triangle BCG \sim \triangle EFG$ with a ratio of $\frac{BC}{EF} = 2$, so $\frac{BG}{GE} = 2$.

Similarly let BE intersect AD at G'. Repeating the above yields $\frac{BG'}{G'E} = 2$. Thus G and G' are the same point, and the medians are concurrent.



■

Corollary 13.13. *Let M be the midpoint of BC. Then the centroid G divides AM into a $2:1$ ratio.*

Exercise 13.14. Prove that the medians divide $\triangle ABC$ into 6 triangles with equal area.

Hint: Triangles $\triangle BGM$ and $\triangle CGM$ have the same height and the same base, so their areas must be equal. On the other hand, $\triangle AMC$ must have triple the area of $\triangle CGM$ due to the centroid ratio: their bases are the same but by similar triangles, the ratio of the height from A to BC to the height from G to BC is equal to the ratio of AM to GM.

§13.1.3 Incenter

Definition 13.15. Let A, B, and C be points in the plane. The **internal angle bisector** of angle $\angle BAC$ is the locus of points D such that D lies inside the angle $\angle BAC$ (i.e. B and C are on opposite sides of line AD) and the distances from D to AB and AC are equal.

We refer to the internal angle bisector when we say angle bisector unless otherwise specified (there also exists an external angle bisector, which we will not talk about in this handout).

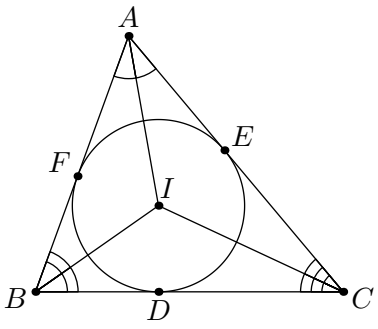
Exercise 13.16. Show that every point D lying on the angle bisector of an angle $\angle ABC$ must satisfy the relation $\angle BAD = \angle DAC$.

Hint: Congruent triangles are helpful.

Exercise 13.17. Show that the angle bisector of an angle $\angle BAC$ must be a line.

Hint: To show that an angle bisector of $\angle ABC$ is a line, fix a point D on it and show that any other point on the angle bisector must lie on line AD.

Theorem 13.18 (Incenter)**.** *In a triangle $\triangle ABC$, the internal angle bisectors of $\angle BAC$, $\angle ACB$, and $\angle CBA$ meet at a point I, the **incenter** of the triangle.*



Definition 13.19. Let the incircle of $\triangle ABC$ touch BC at D. Then D is the ***A*-intouch point**, and the triangle formed by the A-intouch point and the similarly defined B- and C-intouch points is the **contact triangle** or **intouch triangle** of $\triangle ABC$.

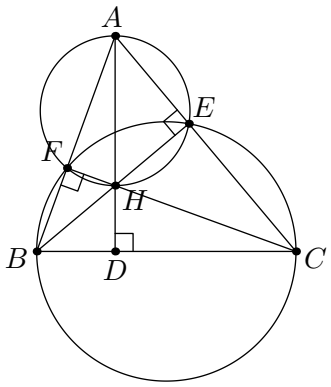
Lemma 13.20. *Let the incircle of $\triangle ABC$ be tangent to BC, CA, and AB at D, E, and F, respectively. Then $AE = AF = s - a$, $BF = BD = s - b$, and $CD = CE = s - c$.*

Exercise 13.21. Prove that $AE = AF = s - a$.

Hint: Using the fact that the tangents from a point to a circle are equal, set $x = AE = AF, y = BF = BD, z = CD = CE$, and solve the resulting system of 3 equations for x, y, z.

§13.1.4 Orthocenter

Definition 13.22. Let A, B, C be points in the plane. The ***A*-altitude** of $\triangle ABC$ is the line passing through A perpendicular to BC. We call the **foot** of the A-altitude the point where the A-altitude intersects BC.



Definition 13.23. In $\triangle ABC$, if D, E, and F are the feet of the altitudes from A, B, and C, respectively, then $\triangle DEF$ is the **orthic triangle** of $\triangle ABC$.

Proposition 13.24. *Let D, E, and F be the feet of the altitudes from A, B, and C, respectively. Then $BCEF$, $CAFD$, and $ABDE$ are cyclic quadrilaterals.*

Exercise 13.25. Prove that $BCEF$ is cyclic; the other two follow from symmetry.

Theorem 13.26. *In a triangle $\triangle ABC$, the A-altitude, B-altitude, and C-altitude meet at a point H, the **orthocenter** of the triangle.*

Exercise 13.27. Let the feet from the A-, B-, and C-altitudes be D, E, and F, respectively. If the B- and C-altitudes meet at H, then prove that $AEHF$ is cyclic.

Exercise 13.28. Prove that the altitudes concur at a point H.

Hint: At this point it should sound like a broken record. Let the B- and C- altitudes meet at H, then use the previous exercise along with some angle chasing to show that A, H', D must be collinear.

§13.1.5 Examples

We begin with a nice lemma that is often a convenient shortcut.

Lemma 13.29. *In triangle $\triangle ABC$, let O, H, and I be the circumcenter, orthocenter, and incenter, respectively. Then*

- *$\angle BOC = 2\angle BAC$ if $\angle BAC$ is acute and $\angle BOC = \pi - 2\angle BAC$ if $\angle BAC$ is obtuse.*
- *$\angle BHC = \pi - \angle BAC$*
- *$\angle BIC = \frac{\pi}{2} + \angle BAC$.*

Proof.

- This follows immediately from the Inscribed Angle Theorem.
- If E and F are the feet of the altitudes from B and C, this follows immediately from the fact that $AEHF$ is cyclic.
- Since $\angle IBC = \frac{1}{2}\angle ABC$ and $\angle ICB = \frac{1}{2}\angle BCA$, we find that

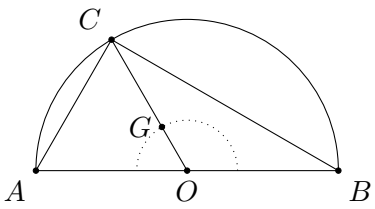
$$\angle BIC = \pi - \angle IBC - \angle ICB = \pi - \left(\frac{\pi}{2} - \angle BAC\right) = \frac{\pi}{2} + \angle BAC.$$

■

Next, we present two applications of the centroid ratio.

Example 13.30 (2018 AMC 10B)**.** Line segment $\overline{AB}$ is a diameter of a circle with $AB = 24$. Point C, not equal to A or B, lies on the circle. As point C moves around the circle, the centroid (center of mass) of $\triangle ABC$ traces out a closed curve missing two points. To the nearest positive integer, what is the area of the region bounded by this curve?

Solution. Let O be the center of the circle and G be the centroid of $\triangle ABC$. Since O is also the midpoint of AB and thus lies on CG, we're motivated to make use of the $2:1$ ratio. CO always has length 12, so it follows that GO always has length 4. This means that the locus of G is a circle with center O and radius 4 by definition, so the area is $16\pi \approx 50$.

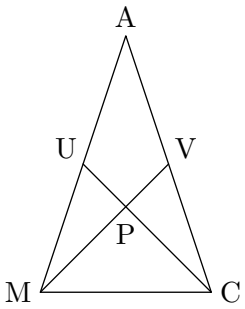


■

Example 13.31 (2020 AMC 10A)**.** Triangle AMC is isoceles with $AM = AC$. Medians $\overline{MV}$ and $\overline{CU}$ are perpendicular to each other, and $MV = CU = 12$. What is the area of $\triangle AMC$?

Solution. Let MV and CU meet at the centroid G and let T be the midpoint of BC. Since $\triangle MTC$ and $\triangle AMC$ share the same base and $GT : AT = 1 : 3$, it suffices to find the area of

$\triangle MTC$ and multiply it by 3. But we know that it is a right triangle and that $MG = CG = \frac{2}{3} \cdot 12 = 8$, so $[AMC] = 3[MTC] = 3 \cdot \frac{8 \cdot 8}{2} = 96$.

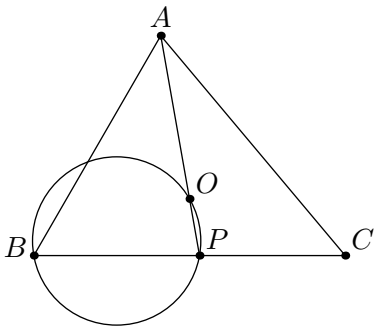


■

Exercise 13.32. In a triangle $\triangle ABC$, show that the B- and C-medians are perpendicular if and only if $b^2 + c^2 = 5a^2$. **Hint:** Use the Pythagorean Theorem.

Example 13.33 (Brazil 2007)**.** Let ABC be a triangle with circumcenter O. Let P be the intersection of straight lines BO and AC and ω be the circumcircle of triangle AOP. Suppose that $BO = AP$ and that the measure of the arc OP in ω, that does not contain A, is $40°$. Determine the measure of the angle $\angle OBC$.

Solution. Note that $BO = AO = AP$, so $\triangle AOP$ is isosceles. Thus $\angle OAP = 20°$, implying $\angle AOC = 140°$, and $\angle AOP = \angle APO = 80°$, implying that $\angle AOB = 100°$. So $\angle OBC = 360° - 140° - 100° = 120°$, or $\angle OBC = 30°$.



■

§13.2 Length Chasing

Often while solving problems we want to find the lengths of unknown line segments in triangles. We do this using a variety of methods.

Theorem 13.34 (Angle Bisector Theorem)**.** *In triangle ABC, let AD be either angle bisector of $\angle BAC$ where D lies on BC. Then we have the following proportion:*

$$\frac{c}{b} = \frac{BD}{CD}.$$

Proof. We prove the theorem for the internal angle bisector only since the external bisector is very similar. First, let's create some similar triangles. Draw a line through B parallel to AD and let its intersection with line AC be E. Then, by AA similarity, we have that EBC is similar to ADC. Because these triangles are similar, we know the following:

$$\frac{a}{DC} = \frac{EC}{b}.$$

Note that $a = BD + DC$, and $EC = EA + b$. Then we can rewrite the proportion as the following:

$$1 + \frac{BD}{DC} = 1 + \frac{EA}{b}.$$

This is starting to look familiar, but... How do we show that $EA = c$? Let's find some angles. By parallel lines, we have that $\angle DAC = \angle BEC$. Further, we have that $\angle BAD = \angle EBA$. Thus since AD is the angle bisector of $\angle BAC$, $\angle AEB = \angle ABE$ so $EA = c$. Thus when we substitute it in,

$$\frac{BD}{CD} = \frac{c}{b}.$$

■

Remark. Notice that with a little further manipulation, we find that $BD = \frac{ac}{b+c}$ and $CD = \frac{ab}{b+c}$. This is very useful too!

The Angle Bisector Theorem is a simple yet instrumental tool in solving geometry problems. Let's try a few examples.

Example (2016 AMC 12A). In $\triangle ABC$, $AB = 6$, $BC = 7$, and $CA = 8$. Point D lies on $\overline{BC}$, and $\overline{AD}$ bisects $\angle BAC$. Point E lies on $\overline{AC}$, and $\overline{BE}$ bisects $\angle ABC$. The bisectors intersect at F. What is the ratio $AF : FD$?

Solution. By the Angle Bisector Theorem applied to $\triangle ABD$, the desired ratio is equal to the ratio of AB to BD. This is a very common trick! Any time you see an angle bisector and a length ratio, the Angle Bisector Theorem should immediately jump out at you.

The application of the theorem will rarely be on the main triangle, so you should always check all the segments the angle bisector intersects before deciding whether or not you should switch to another length chasing method. To finish the problem, we know that $BD = \frac{ac}{b+c} = \frac{7 \cdot 6}{8+6}$, so $\frac{AB}{FD} = \frac{6}{\frac{7 \cdot 6}{8+6}} = 2$, giving us the answer $2 : 1$. ■

Example (2011 AIME). In triangle ABC, $AB = \frac{20}{11}AC$. The angle bisector of $\angle A$ intersects BC at point D, and point M is the midpoint of AD. Let P be the point of the intersection of AC and BM. Find the ratio of CP to PA.

Solution. Okay, there's an angle bisector, so we know that by the Angle Bisector theorem

$$\frac{AB}{AC} = \frac{BD}{DC} = \frac{20}{11}.$$

We can apply this ratio in other ways by applying similar triangles – draw a line through D parallel to BP so that it intersects AC at X. Then DCX is similar to BCP through AA similarity.

This means that $\frac{BC}{DC} = \frac{PC}{XC}$, which in truth means that

$$\frac{BC}{DC} = 1 + \frac{BD}{DC} = 1 + \frac{20}{11} = \frac{PC}{PX} = 1 + \frac{PX}{XC} = \frac{31}{11}.$$

Further, through AA similarity again, we have that AMP is similar to ADX. Thus, since M is the midpoint of AD, P must be the midpoint of AX. Thus $AP = PX$, so the desired ratio $\frac{PC}{PA} = \frac{PC}{PX}$, which is equivalent to

$$\frac{1}{1 - \frac{XC}{PC}} = \frac{1}{1 - \frac{11}{31}} = \frac{31}{20}.$$

■

Exercise 13.35. Let ABC be a right triangle with $\angle ACB = 30$ and $\angle ABC = 90$. Let the angle bisector of $\angle BAC$ intersect BC at D. What is the length of DC, if $AC = 4$?

One of the most important formulas to come up in computational geometry may be Stewart's theorem.

Theorem 13.36 (Stewart's Theorem)**.** *In triangle ABC, let D lie on BC such that AD is a cevian with length d, dividing BC into line segments $BD = m, CD = n$. Then the following holds: $b^2m + c^2n = a(d^2 + mn)$.*

Remark. Stewart's theorem is commonly remembered mnemonically in the form

$$man + dad = bmb + cnc,$$

which corresponds to "a man and his dad put a bomb in the sink."

As you can imagine, this definitely comes in handy while lengths chasing in problems.

Example (2013 AMC 10A)**.** In $\triangle ABC$, $AB = 86$, and $AC = 97$. A circle with center A and radius AB intersects $\overline{BC}$ at points B and X. Moreover $\overline{BX}$ and $\overline{CX}$ have integer lengths. What is BC?

Solution. Since BX and CX have integer lengths, it may be possible to use Stewart's theorem on this problem. Note that $AX = AB = 86$, the radius of the circle, and $AC = 97$. Then let $BX = b$ and $CX = c$. Then by Stewart's theorem,

$$bc(b + c) + 86^2 \cdot (b + c) = 97^2 \cdot b + 86^2 \cdot c.$$

When we simplify and combine like terms, we get the following:

$$b^2c + c^2b = (97^2 - 86^2)b.$$

Since b is nonzero, we can divide both sides by b to get

$$bc + c^2 = c(b + c) = 97^2 - 86^2 = (97 + 86)(97 - 86) = 11 \cdot 61 \cdot 3.$$

By the triangle inequality, $BC < AC + AB$, $BC < 86 + 97$, so $BC < 183$. Since $c < b + c$, c must equal 33 and $b + c = 61$. Thus $BC = 61$, as desired. ■

Exercise 13.37. In triangle $\triangle ABC$, let M be the midpoint of BC. Prove that

$$AM = \sqrt{\frac{2c^2 + 2b^2 - a^2}{4}}.$$

Exercise 13.38. In triangle $\triangle ABC$, let D be the intersection of the angle bisector of $\angle BAC$ with BC. Prove that

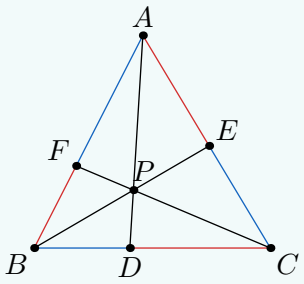
$$AD = \sqrt{\frac{(a+b+c)(b+c-a)bc}{(b+c)^2}}$$

Hint: Use $BD = \frac{ac}{b+c}$ and $CD = \frac{ab}{b+c}$.

Finally, we have a lesser-used, but still important, result:

Theorem 13.39 (Ceva's Theorem). *Given a triangle $\triangle ABC$, let points D, E, F be on lines BC, CA, AB, respectively. If we further require that either all three points lie inside the triangle or two points lie outside the triangle and one lies inside, then AD, BE, CF concur at a single point if and only if*

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1.$$



Exercise 13.40 (AoPS). Suppose AB, AC, and BC have lengths $13, 14$, and 15, respectively. If $\frac{AF}{FB} = \frac{2}{5}$ and $\frac{CE}{EA} = \frac{5}{8}$, find BD and DC.

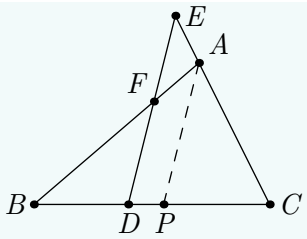
Exercise 13.41. Show that the medians, angle bisectors, and altitudes of a triangle all concur at three respective points (the centroid, incenter, and orthocenter) using Ceva.

Exercise 13.42. Let the incircle of $\triangle ABC$ touch BC, CA, and AB at D, E, and F, respectively. Prove that AD, BE, CF concur at a point known as the **Gergonne Point** of $\triangle ABC$.

The other two cases for where the points D, E, F lie with respect to the triangle $\triangle ABC$ are covered by the following analogous theorem.

Theorem 13.43 (Menelaus's Theorem). *Given a triangle $\triangle ABC$, let D, E, F be on lines BC, CA, AB, respectively. If we further require that all three points lie outside the triangle or two points lie inside the triangle and one lies outside, then D, E, F are collinear if and only if*

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1.$$



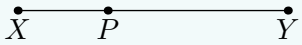
§13.3 Mass Points

Mass points involves assigning weights or a "mass" to points using the ratio of lengths relating the vertices. If we imagine the line segments as having a certain ratio, then the ratio between the weights will be inversely proportional.

Consider a seesaw along line segment AB such that the fulcrum is at point C where $AC = 3$, $BC = 7$. Then, since the ratio of AC to BC is 3 to 7, we can assign the shorter line segment with weight 7 at point A and the longer line segment with weight 3 at point B. Hence, points A and B have a "mass" that represents the ratio $AC : BC$. Further, since C is the fulcrum, or balancing point, C has a mass of the other two points: $3 + 7 = 10$.

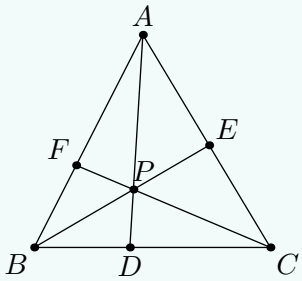
Here's the rigorous definition of mass points.

Theorem 13.44 (Mass Points). *Consider segment XY with P on XY. Then assign masses $\diamond X, \diamond Y$ to points X, Y such that $\frac{XP}{YP} = \frac{\diamond Y}{\diamond X}$.*



Now consider cevians AD, BE, CF of $\triangle ABC$ that concur at some point P. Then $\frac{AP}{PD} = \frac{\diamond B + \diamond C}{\diamond A}$.

This means that for P on XY, we can define $\diamond P = \diamond X + \diamond Y$.



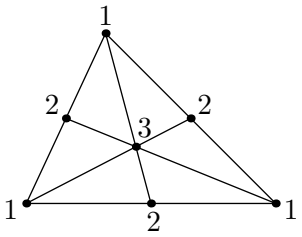
From here we can proceed to derive many properties. This technique can prove to be extremely useful with geometry problems involving the intersection of several line segments.

As a simple example, we'll present the centroid.

Example (Centroid). Assign masses to $\triangle ABC$, its midpoints, and its centroid.

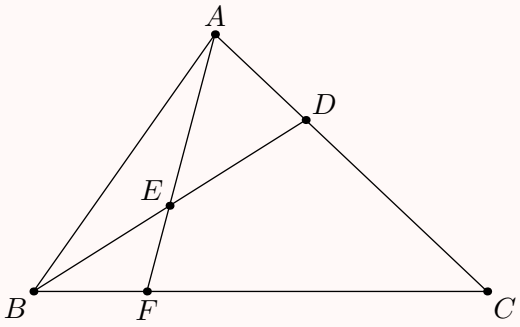
Solution. Note $\diamond A = \diamond B = \diamond C$. Without loss of generality, let $\diamond A = 1$.

Then note that since $\diamond X + \diamond Y = \diamond P$ for P on segment XY, $\diamond D = \diamond B + \diamond C = 2$. Similarly, $\diamond E = \diamond F = 2$, and $\diamond G = \diamond A + \diamond D = 1 + 2 = 3$.



■

Example (2019 AMC 8). In triangle ABC, point D divides side $\overline{AC}$ so that $AD : DC = 1 : 2$. Let E be the midpoint of $\overline{BD}$ and let F be the point of intersection of line BC and line AE. Given that the area of $\triangle ABC$ is 360, what is the area of $\triangle EBF$?



Solution. Since we already know the area of triangle ABC and the ratios of certain lengths, it makes to express the area of EBF, $[EBF]$ in terms of $[ABC]$. First, note that EBF and ABF share the same base, BF. Thus

$$[EBF] = \frac{EF}{AF}[ABF].$$

Further, since ABF and ABC share the same altitude,

$$[ABF] = \frac{BF}{BC}[ABC].$$

Thus, substituting in our expression for $[ABF]$, we have that

$$[EBF] = \frac{EF}{AF} \cdot \frac{BF}{BC}[ABC].$$

This gives us some motivation to proceed with mass points.

Let's start by considering AC. Since $AD : DC = 1 : 2$, we can assign A with a mass of 2 and C with a mass of 1. Then the mass of D is $1 + 2 = 3$. Further, since E is the midpoint of BD, the mass of B is equal to the mass of D, which we already know is 3. Thus, the mass of E is $3 + 3 = 6$. Further, since the mass of B is 3 and the mass of C is 1, we know that F has a mass of $3 + 1 = 4$.

Hence, the ratio of $BF : BC$ is $\frac{1}{4}$. Further, since E has a mass of 6, A has a mass of 2, and F has a mass of 4, the ratio of $EF : AF$ is $\frac{1}{3}$. Substituting these values in, we have that

$$[EBF] = \frac{EF}{AF} \cdot \frac{BF}{BC}[ABC] = \frac{1}{3} \cdot \frac{1}{4} \cdot 360 = 30.$$

■

Example (2011 AIME). In triangle ABC, $AB = \frac{20}{11}AC$. The angle bisector of $\angle A$ intersects BC at point D, and point M is the midpoint of AD. Let P be the point of the intersection of AC and BM. Find the ratio of CP to PA.

Solution. You may recognize this problem from the previous section. This time, we'll use mass points in order to arrive at a faster solution.

Again, we use the Angle Bisector theorem to arrive at the conclusion that

$$\frac{AB}{AC} = \frac{BD}{DC} = \frac{20}{11}.$$

This means that we can assign B a mass of 11 and C a mass of 20, with D having a mass of $11 + 20 = 31$. Then, since M is the midpoint of AD, we have that A has the same mass as D, 31.

Thus we know, when considering the line segment AC, that A has a mass of 31 and C has a mass of 20. Therefore, the ratio of CP to PA is equal to the mass of A over the mass of C, which is $\frac{31}{20}$. ■

This next problem is another instance in which we can apply both the Angle Bisector theorem and mass points.

Example (2009 AIME I). Triangle ABC has $AC = 450$ and $BC = 300$. Points K and L are located on $\overline{AC}$ and $\overline{AB}$ respectively so that $AK = CK$, and $\overline{CL}$ is the angle bisector of angle C. Let P be the point of intersection of $\overline{BK}$ and $\overline{CL}$, and let M be the point on line BK for which K is the midpoint of $\overline{PM}$. If $AM = 180$, find LP.

Solution. First, by the Angle Bisector theorem, we have that

$$\frac{BL}{CB} = \frac{AL}{CA},$$

so when we substitute in $CB = 300$ and $CA = 450$,

$$\frac{BL}{300} = \frac{AL}{450},$$

so $BL = \frac{2}{3}AL$. Thus, we can use mass points and assign A, B, and L weights of $2, 3$, and 5 respectively. Further, since K is the midpoint of AC, C has the same mass, 2, as A. Then, the mass of P must be the combined masses of C and L, which is $2 + 5 = 7$. This means that LP, our desired length, is equivalent to

$$LP = \frac{2}{5}CP.$$

There's just one last step: finding the length of CP. Thankfully, since K is the midpoint of both AC and PM, we know that MKA is congruent to PKC by SAS congruence. This means that $MA = CP = 180$, so

$$LP = \frac{2}{5} \cdot 180 = 72.$$

■

Exercise 13.45 (2016 AMC 12A). In $\triangle ABC$, $AB = 6$, $BC = 7$, and $CA = 8$. Point D lies on $\overline{BC}$, and $\overline{AD}$ bisects $\angle BAC$. Point E lies on $\overline{AC}$, and $\overline{BE}$ bisects $\angle ABC$. The bisectors intersect at F. What is the ratio $AF : FD$?

Exercise 13.46 (2004 AMC 10B). In $\triangle ABC$ points D and E lie on BC and AC, respectively. If AD and BE intersect at T so that $\frac{AT}{DT} = 3$ and $\frac{BT}{ET} = 4$, what is $\frac{CD}{BD}$?

§13.4 Area Formulas Revisited

Area formulas are a simple yet effective way for calculating the area of triangles using the property of circumscribed and inscribed circles.

Theorem 13.47. *For a triangle ABC, $[ABC]$ is equal to $r \cdot s$ where r denotes the radius of the inscribed circle and s denotes the* ***semiperimeter*** *(half of the perimeter).*

Proof. Consider a triangle ABC with a point O that is the center of its inscribed circle. By the definition of an inscribed circle, the perpendicular segments from AB, AC, and BC will intersect at point O. Furthermore, the distance from the point to each segment will be equal to the radius of the inscribed circle.

If we let the radius of the inscribed circle be r, $[ABO]$ is equal to $AB \cdot \frac{r}{2}$. Similarly, $[ACO]$ is equal to $AC \cdot \frac{r}{2}$ and $[BCO]$ is equal to $BC \cdot \frac{r}{2}$. Therefore, the total area of the triangle equals $\frac{(AB+BC+AC)}{2} \cdot r$. ■

Example. If there exists an equilateral triangle ABC such that all three sides have a length of 6, what would be the radius of the inscribed circle? What relation does the radius have with the area of the triangle?

Solution. We can solve this problem using the formula for the area of the equilateral triangle, which gives us $9\sqrt{3}$. The perimeter of the triangle is 18. Plugging this in, the radius of the inscribed circle is $\sqrt{3}$. The area of the triangle can be noted as the product of the radius and the perimeter divided by 2. ■

Example (2004 AMC 10). A triangle with sides of 5, 12, and 13 has both an inscribed and a circumscribed circle. What is the distance between the centers of those circles?

Solution. We can first note that the triangle is a right triangle as (5,12,13) is a pythagorean triple. Let us denote the triangle as ABC with AB, AC, BC respectively being $5, 13$, and 12. The area of the triangle is equal to $5 \cdot \frac{12}{2} = 30$. Using the area formula, we can find the radius of the inscribed circle to be $\frac{30}{15} = 2$.

Let the center of the circumcircle of ABC be point O_1 and the center of the inscribed circle be O_2. Additionally, let us denote the points of intersection between the inscribed circle and AB, AC, BC to be X, Y, and Z, respectively. We can calculate the length of segment of AX by using the property of an inscribed circle. If we denote its length as p, the length of BX is $5 - p$ and BY as well.

Then, CY and CZ are $12 - (5 - p) = p + 7$. Now, we can calculate the length of AZ with the equation of $p + 7 + p = 13$, giving us $p = 3$.

Lastly, the length of ZO_1 is $6.5 - 3 = 3.5$. Using the Pythagorean theorem on $\triangle O_1 Z O_2$ leads to an answer of $\sqrt{16.25}$ or $\frac{\sqrt{65}}{2}$. ■

Exercise 13.48 (2008 AMC 12). Triangle ABC has $AC = 3$, $BC = 4$, and $AB = 5$. Point D is on $\overline{AB}$, and $\overline{CD}$ bisects the right angle. The inscribed circles of $\triangle ADC$ and $\triangle BCD$ have radii r_a and r_b, respectively. What is r_a/r_b?

Another simple yet efficient way of calculating the area of a triangle involves the sine function, where for two sides a, b and an angle $\angle C$ between them, $b \cdot \sin \angle C$ denotes the height of the triangle relative to the side A. Thus, it can be noted that this theorem is a variation of the $\frac{1}{2}bh$ formula where b is the base and h is the height.

Theorem 13.49. *For a triangle ABC, $[ABC]$ is equal to*

$$\frac{1}{2}ab \cdot \sin C.$$

Example. For a triangle ABC with sides AB, BC, AC respectively having lengths of $7, 8$, and 9. The area of the triangle is given to be $\sqrt{720}$. Find $\sin \angle A + \sin \angle B$.

Solution. Using the previous theorem, we can calculate $\sin \angle A$ and $\sin \angle B$.

$$\frac{9 \cdot 7 \sin \angle A}{2} = \sqrt{720}$$

$$\sin \angle A = \frac{\sqrt{720}}{63}$$

We can similarly create an expression for $\sin \angle B$ as the following:

$$\frac{8 \cdot 7 \sin \angle B}{2} = \sqrt{720}$$

$$\sin \angle B = \frac{\sqrt{720}}{56}$$

Adding the two expressions up, we have our answer of

$$\frac{17\sqrt{720}}{504}$$

■

Now we will cover another convenient way of calculating the area of a triangle using the properties of its circumscribed circle. We can rewrite the previous theorem of $[ABC] = \frac{ab}{2} \sin \angle C$ to $\frac{abc}{4R}$ with $\sin \angle C = \frac{c}{2R}$.

Theorem 13.50. *For a triangle ABC, $[ABC] = \frac{A \cdot B \cdot C}{4R}$ where A, B, C are three sides of the triangle and R is the radius of the triangle's circumscribed circle.*

Remark. This theorem is usually paired with the extended law of sines, which we'll go over tomorrow. It will expand on this formula.

Example. For a triangle ABC with AB, BC, and AC respectively having lengths of 3, 8 and 5, develop a generic expression for the radius of circumscribed circle of the triangle using angles $\angle A, \angle B$, and $\angle C$.

Solution. Referring back to the previous theorem, we can note that $[ABC] = \frac{ab}{2} \sin \angle C$ where b represents side AC and a represents BC. Then we can use the Law of Sines to express $b = \frac{a \sin \angle B}{\sin \angle A}$ (if you don't fully understand this step, we'll go over the Law of Sines in detail tomorrow).

Substituting this in gives us $[ABC] = \frac{a^2 \sin \angle B \sin \angle C}{2 \sin \angle A}$. Applying the circumradius formula yields

$$R = \frac{a^2 \sin \angle B \sin \angle C}{240 \sin \angle A}$$

■

Theorem 13.51 (Heron's formula). *The area of a triangle $\triangle ABC$ is*

$$\sqrt{s(s-a)(s-b)(s-c)},$$

where s denotes the semiperimeter.

Remark. This can be proven by splitting the triangle into right triangles, then bashing using the Pythagorean theorem.

Example (2010 AMC 10). A triangle has side lengths 10, 10, and 12. A rectangle has width 4 and area equal to the area of the triangle. What is the perimeter of this rectangle?

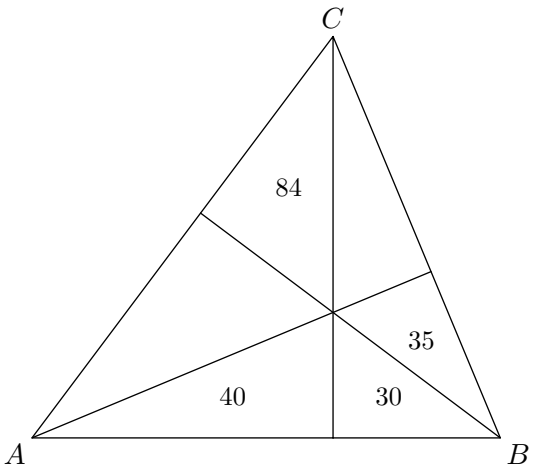
Solution. We can compute the semiperimeter to be 16. Using Heron's Formula, we find that the area of the triangle is $\sqrt{16 \cdot 6 \cdot 6 \cdot 4}$. Since this value equals 48, for the area of the rectangle to equal that of the triangle, its length must be 12. Thus, the perimeter of the rectangle is $2 * (4 + 12) = 32$. ■

Exercise 13.52. Find the area of a triangle with side lengths 13, 14, and 15 using Heron's. What is the circumradius of this triangle? The inradius?

§13.5 Homework Problems

Problem 13.1 (2019 AMC 10A). [4] Let $\triangle ABC$ be an isosceles triangle with $BC = AC$ and $\angle ACB = 40°$. Construct the circle with diameter $\overline{BC}$, and let D and E be the other intersection points of the circle with the sides $\overline{AC}$ and $\overline{AB}$, respectively. Let F be the intersection of the diagonals of the quadrilateral $BCDE$. What is the degree measure of $\angle BFC$?

Problem 13.2 (1985 AIME). [4] As shown in the figure, triangle ABC is divided into six smaller triangles by lines drawn from the vertices through a common interior point. The areas of four of these triangles are as indicated. Find the area of triangle ABC.



Problem 13.3 (2001 AIME)**.** [5] Triangle ABC has $AB = 21$, $AC = 22$ and $BC = 20$. Points D and E are located on $\overline{AB}$ and $\overline{AC}$, respectively, such that $\overline{DE}$ is parallel to $\overline{BC}$ and contains the center of the inscribed circle of triangle ABC. Then $DE = m/n$, where m and n are relatively prime positive integers. Find $m + n$.

Problem 13.4 (2013 AMC 10B)**.** [5] In triangle ABC, medians AD and CE intersect at P, $PE = 1.5$, $PD = 2$, and $DE = 2.5$. What is the area of $AEDC$?

Problem 13.5 (2016 AMC 12A)**.** [5] Let $ABCD$ be a square. Let E, F, G and H be the centers, respectively, of equilateral triangles with bases $\overline{AB}, \overline{BC}, \overline{CD}$, and $\overline{DA}$, each exterior to the square. We can express the ratio of the area of square $EFGH$ to the area of square $ABCD$ as $\frac{a+\sqrt{b}}{c}$ for positive integers a, b, and c where b is squarefree. What is $a + b + c$?

Problem 13.6 (2003 AIME II)**.** [6]

Find the area of rhombus $ABCD$ given that the radii of the circles circumscribed around triangles ABD and ACD are 12.5 and 25, respectively.

Problem 13.7 (2016 AMC 10A)**.** [6] In rectangle $ABCD$, $AB = 6$ and $BC = 3$. Point E between B and C, and point F between E and C are such that $BE = EF = FC$. Segments $\overline{AE}$ and $\overline{AF}$ intersect $\overline{BD}$ at P and Q, respectively. The ratio $BP : PQ : QD$ can be written as $r : s : t$ where the greatest common factor of r, s and t is 1. What is $r + s + t$?

Problem 13.8 (2016 AMC 10B)**.** [7] Rectangle $ABCD$ has $AB = 5$ and $BC = 4$. Point E lies on $\overline{AB}$ so that $EB = 1$, point G lies on $\overline{BC}$ so that $CG = 1$. and point F lies on $\overline{CD}$ so that $DF = 2$. Segments $\overline{AG}$ and $\overline{AC}$ intersect $\overline{EF}$ at Q and P, respectively. We can write the value of $\frac{PQ}{EF}$ as a fraction $\frac{p}{q}$ in lowest terms. What is $p + q$?

Problem 13.9 (2016 AIME I)**.** [7] In $\triangle ABC$ let I be the center of the inscribed circle, and let the bisector of $\angle ACB$ intersect AB at L. The line through C and L intersects the circumscribed circle of $\triangle ABC$ at the two points C and D. If $LI = 2$ and $LD = 3$, then $IC = \frac{p}{q}$, where p and q are relatively prime positive integers. Find $p + q$.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

14 Analytic Geometry + Trigonometric Techniques

§14.1 Coordinate Bashing

You are probably familiar with the Cartesian coordinate plane and its algebraic applications. You know the formulas for line equations, circle equations, conditions for perpendicularity, conditions for parallel lines, etc. Usually, we see these objects in the context of algebra, but seem closely related to many geometrical concepts.

This naturally leads to the question, "Can we use our algebraic techniques in the Cartesian coordinate plane to solve geometry problems?" The answer is in fact yes, and this is the idea behind **coordinate bashing**, or turning a geometry problem into an algebraic one.

We first present three formulas that will help greatly when coordinate bashing:

Proposition 14.1 (Distance Formula). *The distance between two points (x_1, y_1) and (x_2, y_2) is*

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

Exercise 14.2. Prove this!

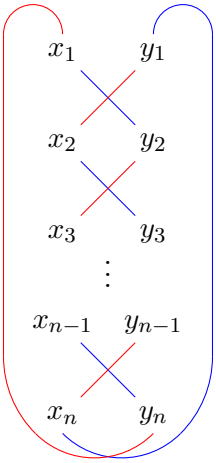
Proposition 14.3 (Point to Line Distance Formula). *The distance between point (x_1, y_1) to line $ax + by + c = 0$ is*

$$\frac{|ax_1 + by_1 + c|}{\sqrt{a^2 + b^2}}.$$

Proposition 14.4 (Shoelace Formula). *Suppose an n-sided convex polygon has vertices at $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$, where the vertices are in counterclockwise or clockwise order. Its area is given by*

$$\frac{1}{2}|(x_1y_2 + x_2y_3 + \cdots + x_ny_1) - (x_2y_1 + x_3y_2 + \cdots x_1y_n)|.$$

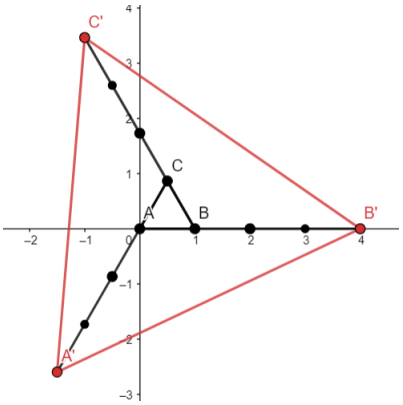
The following diagram shows why it's called the Shoelace Formula. Take half of the absolute value of the products joined by the blue lines and subtract the products joined by the red lines to get the area, as shown in the diagram.



Let's see it in action.

Example 14.5 (2017 AMC 10). Let ABC be an equilateral triangle. Extend side $\overline{AB}$ beyond B to a point B' so that $BB' = 3AB$. Similarly, extend side $\overline{BC}$ beyond C to a point C' so that $CC' = 3BC$, and extend side $\overline{CA}$ beyond A to a point A' so that $AA' = 3CA$. What is the ratio of the area of $\triangle A'B'C'$ to the area of $\triangle ABC$?

Solution. Since this problem is asking for ratios, let's just assume that $\triangle ABC$ has side length of 1. First, we need to find A, B, and C on the coordinate plane. To make life easier, we like to get as many points as possible on the coordinate axes, since at least one of the coordinates will become 0 (we'll see how this reduces calculations). Set one of these points at the origin, say, A. We can then get another point on the coordinate axis: let B be at $(1, 0)$. Finally, since ABC is an equilateral triangle, C will be at a distance of $\frac{\sqrt{3}}{2}$ away from the midpoint of AB. The midpoint of AB is given by $\left(\frac{0+1}{2}, \frac{0+0}{2}\right)$, or $\left(\frac{1}{2}, 0\right)$, so C is at $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$,



Now how do we have A', B', and C'? Well, for each segment, we can phrase it in terms of "rise and run." For example, if we consider AC, we can consider it a "rise" of $\frac{\sqrt{3}}{2}$ and a "run" of $\frac{1}{2}$. However, if we consider CA, which goes in the opposite direction, we consider it a "rise" of $-\frac{\sqrt{3}}{2}$ and a "run" of $-\frac{1}{2}$. Thus, if we extend AC past A to A' so that $AA' = 3CA$, we can think of it as extending CA past A for 3 "rise and runs", or changing the y-coordinate of A by $-\frac{\sqrt{3}}{2}$ three times and changing the x coordinate of A by $-\frac{1}{2}$ three times. Thus, our coordinates for A' are

$$\left(0 + 3\left(-\frac{1}{2}\right), 0 + 3\left(-\frac{\sqrt{3}}{2}\right)\right) = \left(-\frac{3}{2}, -\frac{3\sqrt{3}}{2}\right)$$

Applying similar ideas to find B' and C',

$$B' : (1+3(1), 0+3(0)) = (4,0)$$

$$C' : \left(\frac{1}{2}+3\left(-\frac{1}{2}\right), \frac{\sqrt{3}}{2}+3\left(\frac{\sqrt{3}}{2}\right)\right) = \left(-1, 2\sqrt{3}\right)$$

> *Remark.* The concept of CA and AC being different due to direction is known as *directed lengths*.

All we need to do now is to find the area of $A'B'C'$. This is where we see one of the benefits of coordinate bashing: finding areas is extremely easy once you know the points of the shape. To Shoelace, set your points up as follows:

$$(4,0)$$
$$(-\frac{3}{2}, -\frac{3\sqrt{3}}{2})$$
$$(-1, 2\sqrt{3})$$
$$(4,0)$$

Think about why we chose to start with $(4,0)$. Because we're multiplying a lot, we want as many zeroes as possible to reduce calcuations. Because we put the first point again at the end, we will ideally want the first point to have at least one coordinate be 0. Applying the formula, we get our area to be

$$\frac{1}{2}\left|\left(4\right)\left(-\frac{3\sqrt{3}}{2}\right)+\left(-\frac{3}{2}\right)\left(2\sqrt{3}\right)+(-1)(0)\right)-\left(\left(0\right)\left(-\frac{3}{2}\right)+\left(-\frac{3\sqrt{3}}{2}\right)(-1)+(2\sqrt{3})(4)\right)|$$

$$= \frac{1}{2}|-6\sqrt{3}-3\sqrt{3}-\frac{3\sqrt{3}}{2}-8\sqrt{3}|$$

$$= \frac{1}{2}\left(\frac{37\sqrt{3}}{2}\right) = \frac{37\sqrt{3}}{4}$$

So our area for $A'B'C'$ is $\frac{37\sqrt{3}}{4}$. Since the area of ABC is $\frac{\sqrt{3}}{4}$, the ratio of the areas of $A'B'C'$ to ABC is simply $\boxed{37:1}$. ■

Some takeaways: the "rise and run" idea is *extremely* important, and this will come up over and over again (this is especially true for problems involving reflections). Also, staying organized when coordinate bashing is extremely important! One mistake with a sign or calculation can be your downfall.

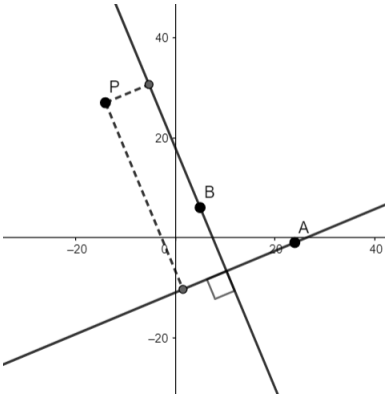
Now, let's look at another advantage that coordinate bashing provides:

Example 14.6. (2011 AIME I) Let L be the line with slope $\frac{5}{12}$ that contains the point $A = (24, -1)$, and let M be the line perpendicular to line L that contains the point $B = (5, 6)$. The original coordinate axes are erased, and line L is made the x-axis, and line M the y-axis. In the new coordinate system, point A is on the positive x-axis, and point B is on the positive y-axis. The point P with coordinates $(-14, 27)$ in the original system has coordinates (α, β) in the new coordinate system. Find $\alpha + \beta$.

Solution. How can we interpret these new coordinates? That is, what does $(1, 2)$ mean in the Cartesian coordinate plane? We know it's the point that is 1 to the right of the y axis, and 2 above the x axis, i.e. it is has (signed) distance 1 from the y axis and a distance of 2 from the x axis.

So what is (α, β) really asking for? It's asking for the distance from the new rotated x and y axes! Of course, we need to remember positive and negative is significant, but that won't be too difficult as we just need to check if the point is above/below the new axes.

This is where coordinate bashing provides a significant advantage, because we literally have a formula for finding the distance between points and lines. So let's compute this!



First, we need to find our equations for our lines in standard form ($ax + by + c = 0$). Using point-slope,

$$L : (y + 1) = \frac{5}{12}(x - 24) \iff 5x - 12y - 132 = 0$$

$$M : (y - 6) = -\frac{12}{5}(x - 5) \iff 12x + 5y - 90 = 0$$

Using our point line distance formula, we can find the distance between P and each of L and M! Let the distance between point X and line L be denoted as $d(X, L)$:

$$d(P, L) = \frac{|5(-14) - 12(27) - 132|}{\sqrt{5^2 + 12^2}} = \frac{526}{13}$$

$$d(P, M) = \frac{|12(-14) + 5(27) - 90|}{\sqrt{5^2 + 12^2}} = \frac{123}{13}$$

So we now know that P is of the form $\left(\pm\frac{123}{13}, \pm\frac{526}{13}\right)$ and it suffices to figure out the signs. Remember that the distance from the x axis is the absolute value of the y-coordinate, and vice versa! Don't mix these up!

Let's find the x coordinate first: if A is on the positive x axis, then anything on the same side of the y axis, M, will have a positive x coordinate. To check which side A is on compared to M, we can easily see that $12(24) + 5(-1) - 90 > 0$. Thus, if we get a positive value when we plug in P into the equation, then the x coordinate will be positive, and vice versa:

$$12(-14) + 5(27) - 90 = -168 + 135 - 90 < 0$$

Since our value is negative, P lies on the opposite side of M as A, meaning the x coordinate is negative.

We follow a similar process to find the sign of the y coordinate. First, plug in B into the L to get that $5(5) - 12(6) - 132 < 0$. Thus, if we plug in P and get a negative value, P will lie on the same side of L as B, meaning the y coordinate is positive, and vice versa:

$$5(14) - 12(27) - 132 < 0$$

This means our y coordinate is positive, so our point P is $\left(-\frac{123}{13}, \frac{526}{13}\right)$, meaning our answer is $-\frac{123}{13} + \frac{526}{13} = \frac{403}{13} = \boxed{31}$. ■

Remark. For those of you preparing for the AIME, this problem appeared very early and is very difficult for its position. If you are running out of time and you have gotten to $P = \left(\pm\frac{123}{13}, \pm\frac{526}{13}\right)$, you can take advantage of the fact that answers for the AIME are positive integers, so you just need to check $\frac{526+123}{13}$ and $\frac{526-123}{13}$, of which only the latter gives an integer.

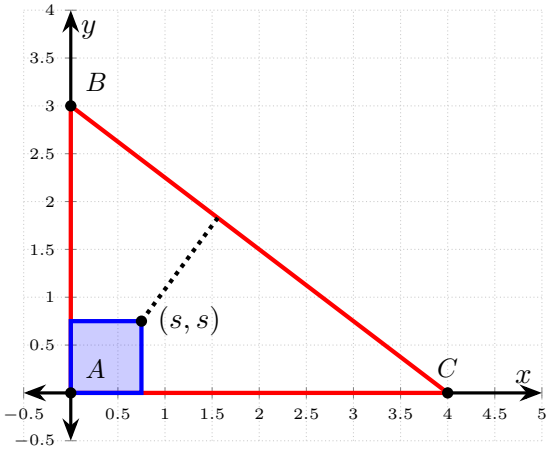
Now let's finish with one more example, which shows an application of using coordinate bashing to *find points* and solve equations, rather than straight computation.

Example 14.7. (2018 AMC 10A) Farmer Pythagoras has a field in the shape of a right triangle. The right triangle's legs have lengths 3 and 4 units. In the corner where those sides meet at a right angle, he leaves a small unplanted square S so that from the air it looks like the right angle symbol. The rest of the field is planted. The shortest distance from S to the hypotenuse is 2 units. What fraction of the field is planted?

Solution. You've seen this example before, but this time we'll do it with coordinates.

In order to find the fraction of the field that is planted, we need to find the part that is unplanted. Since this is just a square, all we need is the side length, s. How can we set this up with coordinates?

We want to take advantage of the fact that its a right triangle: because the x and y axes are perpendicular, its natural to place the right triangle in the plane such that its vertex is at the origin $(0, 0)$ and the other two points are on the axes (so that the legs coincide with each axis). Let these points be $(0, 3)$ and $(4, 0)$. Remember, we want to get as many zeroes as possible!



So how could we find the side length of the square? Let's use the piece of information we haven't used yet: the shortest distance from the square S to the hypotenuse is 2 units. This means that the point diagonally opposite the vertex will be a distance 2 away from the hypotenuse.

Aha! If we can represent this point in terms of variables, we can just plug it into the distance formula to solve for the point! This is where the square comes into play: let the side length of the square be s. The point diagonally opposite the vertex then is simply (s, s) (convince yourself of this!).

To use the distance formula, we need our line equation. The slope is just $\frac{-3}{4}$, and we know the y-intercept is $(0, 3)$, so our equation is

$$y = -\frac{3}{4}x + 3 \iff 3x + 4y - 12 = 0$$

Plugging in (s, s) into our distance formula and setting the value equal to 2,

$$\frac{|3s + 4s - 12|}{\sqrt{3^2 + 4^2}} = 2 \implies |7s - 12| = 10 \implies s = \frac{22}{7}, \frac{2}{7}$$

Which value of s do we use? Well, $\frac{22}{7} > 3$, which means that part of the square will actually lie outside of the triangle, which is not right (essentially, it's too big). Thus, $s = \frac{2}{7}$, or the area of our triangle is $\left(\frac{2}{7}\right)^2 = \frac{4}{49}$. Since the area of our triangle is $\frac{3 \cdot 4}{2} = 6$, the fraction of the square that is *unplanted* is $\frac{4}{49 \cdot 6} = \frac{2}{147}$, so the fraction of the square that is planted is $1 - \frac{2}{147} = \boxed{\frac{145}{147}}$. ■

Hopefully these examples give you a good sense of the power coordinate bashing provides. However, use this technique sparingly! It can get computationally intense, and is prone to mistakes. In general, use this technique only if there are lots of perpendicular lines/right angles or triangles (points of quadrilaterals can get difficult to find), and if the question asks to find distances or areas.

If you are familiar with equations of circles, feel free to use this as well! Although we won't cover it in this handout, we will list some things to keep in mind with circles:

- Generally, try to keep it to one circle: you should never go over two.
- Tangency to lines is always nice, because the radius will be equal to the distance from the point to the respective line, so using one of the axes as the line will give you a free coordinate
- Remember that if you intersect a line with a circle, you will (usually) have two intersection points: never forget about the other!
- If you decide to use two circles and have a problem dealing with the line through the two intersections, you can actually find the equation of the line by *subtracting* the circle equations (although this isn't common, it's extremely useful when it does show up)

Exercise 14.8 (2015 AMC 10A). The isosceles right triangle ABC has right angle at C and area 12.5. The rays trisecting $\angle ACB$ intersect AB at D and E. What is the area of $\triangle CDE$?

Exercise 14.9 (2019 AMC 10B). Rectangle $ABCD$ has $AB = 5$ and $BC = 4$. Point E lies on $\overline{AB}$ so that $EB = 1$, point G lies on $\overline{BC}$ so that $CG = 1$, and point F lies on $\overline{CD}$ so that $DF = 2$. Segments $\overline{AG}$ and $\overline{AC}$ intersect $\overline{EF}$ at Q and P, respectively. What is the value of $\frac{PQ}{EF}$?

§14.2 Law of Sines

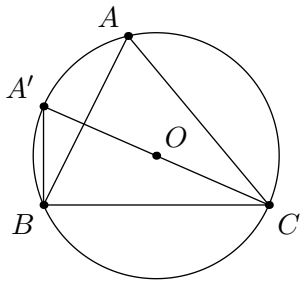
Theorem 14.10. *In triangle $\triangle ABC$ with circumradius R, we have*

$$\frac{a}{\sin\angle CAB} = \frac{b}{\sin\angle ABC} = \frac{c}{\sin\angle BCA} = 2R.$$

Proof. Let M be the midpoint of BC and let O be the circumcenter of $\triangle ABC$. We will just show that $\frac{a}{\sin\angle CAB} = 2R$, since we can prove that $\frac{b}{\sin\angle ABC} = 2R$ and $\frac{c}{\sin\angle BCA} = 2R$ in the exact same way. If $\angle BAC$ is right, the circumcenter is the midpoint of the hypotenuse, so $2R = a$ and $\cos\angle CAB = \cos\frac{\pi}{2} = 1$, which immediately implies $\frac{a}{\sin\angle CAB} = 2R$. If $\angle BAC$ is acute, by the Inscribed Angle Theorem, we must have $\angle BOC = 2\angle CAB$, so by definition,

$$\sin\angle CAB = \sin\angle BOM = \frac{BM}{BO} = \frac{\frac{a}{2}}{R},$$

which becomes $\frac{a}{\sin\angle CAB} = 2R$ as desired. In the case where $\angle CAB$ is obtuse, we instead have $\angle BOC = 2\pi - 2\angle CAB$, so $\sin\angle BOM = \sin(\pi - \angle CAB) = \sin\angle CAB$, which gives the same result.



■

Example 14.11 (2005 AIME II/14). In triangle $ABC, AB = 13, BC = 15$, and $CA = 14$. Point D is on $\overline{BC}$ with $CD = 6$. Point E is on $\overline{BC}$ such that $\angle BAE \cong \angle CAD$. Given that $BE = \frac{p}{q}$ where p and q are relatively prime positive integers, find q.

Solution. This is very straightforward. We find that

$$\begin{aligned}
BE &= \frac{AB\sin\angle BAE}{\sin\angle AEB} && \text{(Law of Sines on } \triangle ABE\text{)}\\
&= \frac{AB\sin\angle BAE}{\sin\angle AEC} && (\angle AEB = \pi - \angle AEC)\\
&= \frac{AB\cdot CE\sin\angle BAE}{AC\sin\angle CAE} && \text{(Law of Sines on } \triangle AEC\text{)}\\
&= \frac{AB\cdot CE\sin\angle BAE}{AC\sin\angle BAD} && (\angle CAE = \angle BAD)\\
&= \frac{AB^2\cdot CE\sin\angle BAE}{AC\cdot BD\sin\angle BDA} && \text{(Law of Sines on } \triangle BAD\text{)}\\
&= \frac{AB^2\cdot CE\sin\angle BAE}{AC\cdot BD\sin\angle CDA} && (\angle BDA = \pi - \angle CDA)\\
&= \frac{AB^2\cdot CE\cdot CD\sin\angle BAE}{AC^2\cdot BD\sin\angle CAD} && \text{(Law of Sines on } \triangle CAD\text{)}\\
&= \frac{13^2\cdot(15-BE)\cdot 6}{14^2\cdot 9},
\end{aligned}$$

so $BE = \frac{13^2\cdot 15}{463} \implies q = \boxed{463}$. ■

We pretty much solved this problem just by continuously substituting sines with either the Law of Sines or the given angle equalities, with little geometric or even algebraic cleverness involved. The main reason why this worked was because we already had most of lengths in the problem and thus substituting sines didn't result in new unknowns, but usually this is not the case. In the next example, we will have to construct an auxiliary point, though it is rather easily motivated.

Example 14.12 (2019 PUMAC). Let $\triangle ABC$ be a triangle with circumcenter O and orthocenter H. Let D be a point on the circumcircle of ABC such that $AD \perp BC$. Suppose that $AB = 6$, $DB = 2$, and the ratio $\frac{\text{area}(\triangle ABC)}{\text{area}(\triangle HBC)} = 5$. Then, if OA is the length of the circumradius, then OA^2 can be written in the form $\frac{m}{n}$, where m, n are relatively prime positive integers. Compute $m + n$.

Solution. Let $AO = R$ as usual. Since O isn't explicitly connected to anything in the problem, it's probably a good idea to use the Law of Sines to find R. By cyclic quadrilaterals, $\angle BCA = \angle BDA$, so

$$2R = \frac{6}{\sin \angle BCA} = \frac{6}{\sin \angle BDA},$$

and thus it suffices to find $\sin \angle BDA$. Well, we know that $AD \perp BC$, so we are motivated to let D' be the foot of the altitude from A to BC. By the given area ratio and orthocenter reflections, we can set $HD' = DD' = x$ and $AH = 4x$. Now we just want x, which we can find with the Pythagorean Theorem:

$$6^2 - (5x)^2 = BD'^2 = 2^2 - x^2 \implies x = \sqrt{\frac{4}{3}}, BD' = \sqrt{\frac{8}{3}}.$$

We've found all the lengths we need, and at this point the problem is just computation:

$$R^2 = \left(\frac{6}{2\sin \angle BDA}\right)^2 = \left(\frac{3BD}{BD'}\right)^2 = \left(\frac{6}{\sqrt{\frac{8}{3}}}\right)^2 = \left(\sqrt{\frac{27}{2}}\right)^2,$$

so $\boxed{29}$ is our desired answer. ■

Although the symmetric sine equality is certainly pretty useful as we saw in our first example, the Law of Sines really shines when we want to find the circumradius; any time you see the circumradius **even mentioned**, you should immediately consider the Law of Sines. However, the Law of Sines obviously can't solve *every* circumradius problem (efficiently at least), so try not to go down a trig bash rabbit hole. Using the Law of Sines, we can also prove a generalization of the Angle Bisector Theorem.

Lemma 14.13 (Ratio Lemma). *In $\triangle ABC$, let D be a point on A. Then*

$$\frac{BD}{CD} = \frac{c}{b} \cdot \frac{\sin \angle CAD}{\sin \angle BAD}.$$

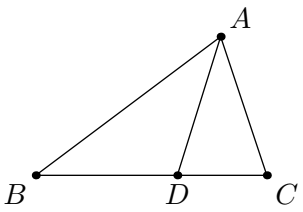
Proof. By the Law of Sines on $\triangle ABD, \triangle ACD$, we know that

$$\frac{BD}{\sin \angle BAD} = \frac{c}{\sin \angle ADB}, \frac{CD}{\sin \angle CAD} = \frac{b}{\sin \angle ADC},$$

respectively. Dividing the first equation by the second, we get

$$\begin{aligned}\frac{BD}{CD}\cdot\frac{\sin\angle BAD}{\sin\angle CAD}&=\frac{c}{b}\cdot\frac{\sin\angle ADB}{\sin\angle ADC}\\ \frac{BD}{CD}&=\frac{c}{b}\cdot\frac{\sin\angle ADB}{\sin(\pi-\angle ADB)}\cdot\frac{\sin\angle CAD}{\sin\angle BAD}\\ \frac{BD}{CD}&=\frac{c}{b}\cdot\frac{\sin\angle CAD}{\sin\angle BAD}\end{aligned}$$

as desired.



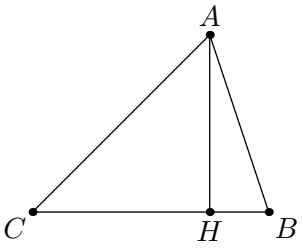
■

§14.3 Law of Cosines

Theorem 14.14 (Law of Cosines). *In triangle ABC, we have that*

$$c^2=a^2+b^2-2ab\cos\angle ACB.$$

Proof. Let the foot of the altitude from A to BC be H. Then note that $A=b\sin C$, $CH=b\cos C$, and $BH=|a-b\cos C|$. (The absolute value is because $\angle B$ can either be acute or obtuse.) Then note by the Pythagorean Theorem, $(b\sin C)^2+(a-b\cos C)^2=a^2+b^2-2ab\cos C=c^2$.



■

We can use the Law of Cosines to prove a very handy formula from the previous handout!

Example. Prove Stewart's theorem using Law of Cosines.

Solution. We start off with triangle ABC such that D lies on BC with AD a cevian with length d, dividing BC into line segments $BD=m, CD=n$. Then we can apply Law of Cosines to both ACD and ABD. In ACD, $AC^2=DC^2+AD^2-2\cdot AD\cdot DC\cos ADC$ corresponds to

$$b^2=d^2+n^2-2dn\cos ADC.$$

Similarly, we apply the same method to ABD to obtain

$$c^2 = d^2 + m^2 - 2dm\cos ADB.$$

Note that $\cos ADB = -\cos ADC$ because $\angle ADB$ and $\angle ADC$ are supplementary. Then, solving for $\cos ADC$ in two ways, we have that

$$\cos ADC = \frac{d^2 + n^2 - b^2}{2dn} = \frac{c^2 - d^2 - m^2}{2dm}.$$

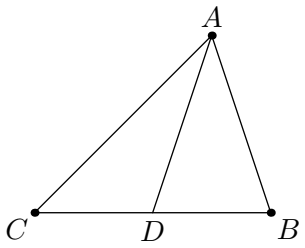
Once we cross multiply and simplify a bit, we have that

$$c^2 n + b^2 m = m^2 n + n^2 m + d^2 m + d^2 n.$$

Factoring the right hand side of the equation yields $mn(m+n)+d^2(m+n)$, so we can substitute $a = m + n$ to finally obtain

$$c^2 n + b^2 m = a(mn + d^2),$$

as desired.



■

Now let's apply Law of Cosines to some competition questions.

Example (2012 AMC 12A). Circle C_1 has its center O lying on circle C_2. The two circles meet at X and Y. Point Z in the exterior of C_1 lies on circle C_2 and $XZ = 13$, $OZ = 11$, and $YZ = 7$. What is the radius of circle C_1?

Solution. We want to find r, the radius of C_1. Note that $XO = OY = r$. We could either apply Law of Cosines on YZO or OZX, except for one issue: how do we find the cosine of $\angle YZO$ or $\angle OZX$, respectively?

One of the key things to note with this problem is that $XOYZ$ is a cyclic quadrilateral. It's important to note that $\angle YZO = \angle YXO$, and we can find $\cos YXO$ due to XOY being isoceles – all we need to obtain is the ratio of

$$\frac{\frac{1}{2}XY}{r}.$$

Thus, we can try to use Ptolemy's theorem to help find our desired ratios. By Ptolemy's theorem applied to $XOYZ$,

$$11 \cdot XY = 7r + 13r = 20r,$$

so $XY = \frac{20}{11}r$. Thus,

$$\cos YZO = \cos YXO = \frac{\frac{1}{2}XY}{r} = \frac{10}{11}.$$

Success! Now we can apply Law of Cosines to obtain our desired length:

$$r^2 = 11^2 + 7^2 - 2 \cdot 11 \cdot 7 \cdot \frac{10}{11} = 30,$$

so $r = \sqrt{30}$. ■

Example (2012 AIME I). Let $\triangle ABC$ be a right triangle with right angle at C. Let D and E be points on $\overline{AB}$ with D between A and E such that $\overline{CD}$ and $\overline{CE}$ trisect $\angle C$. If $\frac{DE}{BE} = \frac{8}{15}$, then find $\tan B$.

Solution. First, let's note that $\tan B = \frac{AC}{BC}$. Since this problem is concerned with the ratio of lengths and not lengths-chasing, without loss of generality we can set $BC = 1$. Since CD and CE trisect $\angle C$, we also have angle bisectors – which is important because we can then apply the Angle Bisector Theorem. Another great thing about the trisectors of this right angle is that it splits $\angle C$ into angles that we can easily calculate the cosine of – $90, 60, 30$, etc. Since $\frac{DE}{BE} = \frac{8}{15}$,

$$DC = \frac{8}{15} \cdot BC = \frac{8}{15}.$$

Now we can apply Law of Cosines to BDC :

$$BD^2 = \left(\frac{8}{15}\right)^2 + 1 - 2 \cdot \frac{8}{15} \cdot 1 \cdot \cos 60 = \frac{169}{225}.$$

Thus $BD = \frac{13}{15}$. Now we can obtain the cosine of $\angle B$, and from there, use that value to obtain the sine of $\angle B$. Since $\tan B = \frac{\sin B}{\cos B}$, we can then get our desired answer. We apply Law of Cosines again to BDC :

$$\frac{64}{225} = 1^2 + \frac{169}{225} - 2 \cdot 1 \cdot \frac{13}{15} \cdot \cos B.$$

Solving for

$$\cos B = \frac{1 + \frac{169}{225} - \frac{64}{225}}{\frac{26}{15}}$$

yields us $\frac{11}{13}$. Then we can solve for

$$\sin B = \sqrt{1 - \cos^2 B} = \sqrt{1 - \frac{121}{169}} = \frac{4\sqrt{3}}{13}.$$

Finally,

$$\tan B = \frac{\sin B}{\cos B} = \frac{4\sqrt{3}}{11}.$$

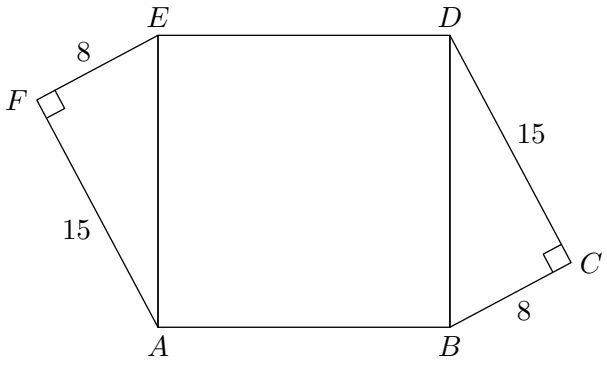
■

Exercise 14.15. Let $ABCDEF$ be a regular hexagon with side length 4. Let M be the midpoint of side AB. Then find the length of MC.

Exercise 14.16 (2006 AMC 12B). Isosceles $\triangle ABC$ has a right angle at C. Point P is inside $\triangle ABC$, such that $PA = 11$, $PB = 7$, and $PC = 6$. Legs $\overline{AC}$ and $\overline{BC}$ have length $s = \sqrt{a + b\sqrt{2}}$, where a and b are positive integers. What is $a + b$?

§14.4 Homework Problems

Problem 14.1 (2015 PUMaC B Division)**.** [3] Find the distance $\overline{CF}$ in the diagram below where $ABDE$ is a square and angles and lengths are as given:



The length $\overline{CF}$ is of the form $a\sqrt{b}$ for integers a, b such that no integer square greater than 1 divides b. What is $a + b$?

Problem 14.2 (2001 AIME I)**.** [4] In triangle ABC, angles A and B measure 60 degrees and 45 degrees, respectively. The bisector of angle A intersects $\overline{BC}$ at T, and $AT = 24$. The area of triangle ABC can be written in the form $a + b\sqrt{c}$, where a, b, and c are positive integers, and c is not divisible by the square of any prime. Find $a + b + c$.

Problem 14.3 (2020 AMC 10A)**.** [5] Quadrilateral $ABCD$ satisfies $\angle ABC = \angle ACD = 90°, AC = 20$, and $CD = 30$. Diagonals $\overline{AC}$ and $\overline{BD}$ intersect at point E, and $AE = 5$. What is the area of quadrilateral $ABCD$?

Problem 14.4 (1971 AHSME)**.** [5] Quadrilateral $ABCD$ is inscribed in a circle with side AD, a diameter of length 4. If sides AB and BC each have length 1, then side CD has length $\frac{p}{q}$, where p and q are positive coprime integers. What is the value of $p + q$?

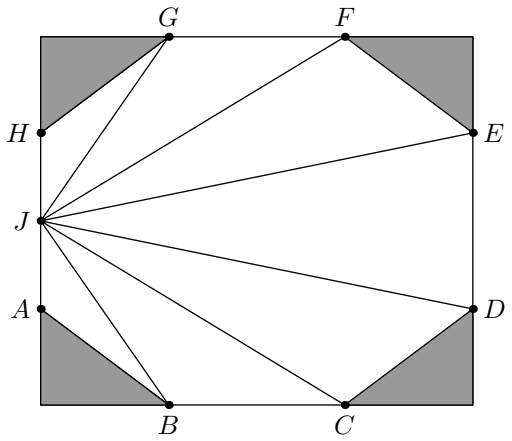
Problem 14.5 (2017 AIME II)**.** [7] Rectangle $ABCD$ has side lengths $AB = 84$ and $AD = 42$. Point M is the midpoint of $\overline{AD}$, point N is the trisection point of $\overline{AB}$ closer to A, and point O is the intersection of $\overline{CM}$ and $\overline{DN}$. Point P lies on the quadrilateral $BCON$, and $\overline{BP}$ bisects the area of $BCON$. Find the area of $\triangle CDP$.

Problem 14.6 (2010 AIME II)**.** [7] Let $ABCDEF$ be a regular hexagon. Let G, H, I, J, K, and L be the midpoints of sides AB, BC, CD, DE, EF, and AF, respectively. The segments $\overline{AH}$, $\overline{BI}$, $\overline{CJ}$, $\overline{DK}$, $\overline{EL}$, and $\overline{FG}$ bound a smaller regular hexagon. Let the ratio of the area of the smaller hexagon to the area of $ABCDEF$ be expressed as a fraction $\frac{m}{n}$ where m and n are relatively prime positive integers. Find $m + n$.

Problem 14.7 (2013 AIME II)**.** [7] In $\triangle ABC$, $AC = BC$, and point D is on $\overline{BC}$ so that $CD = 3 \cdot BD$. Let E be the midpoint of $\overline{AD}$. Given that $CE = \sqrt{7}$ and $BE = 3$, the area of $\triangle ABC$ can be expressed in the form $m\sqrt{n}$, where m and n are positive integers and n is not divisible by the square of any prime. Find $m + n$.

Problem 14.8 (2019 AIME I)**.** [10] Triangle ABC has side lengths $AB = 4$, $BC = 5$, and $CA = 6$. Points D and E are on ray AB with $AB < AD < AE$. The point $F \neq C$ is a point of intersection of the circumcircles of $\triangle ACD$ and $\triangle EBC$ satisfying $DF = 2$ and $EF = 7$. Then BE can be expressed as $\frac{a+b\sqrt{c}}{d}$, where a, b, c, and d are positive integers such that a and d are relatively prime, and c is not divisible by the square of any prime. Find $a + b + c + d$.

Problem 14.9 (2018 AIME II)**.** [7] Octagon $ABCDEFGH$ with side lengths $AB = CD = EF = GH = 10$ and $BC = DE = FG = HA = 11$ is formed by removing four $6 - 8 - 10$ triangles from the corners of a 23×27 rectangle with side $\overline{AH}$ on a short side of the rectangle, as shown. Let J be the midpoint of $\overline{HA}$, and partition the octagon into 7 triangles by drawing segments $\overline{JB}$, $\overline{JC}$, $\overline{JD}$, $\overline{JE}$, $\overline{JF}$, and $\overline{JG}$. Find the area of the convex polygon whose vertices are the centroids of these 7 triangles.



Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

Hint: The centroid of the triangle with vertices $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ is $\left(\frac{x_1+x_2+x_3}{3}, \frac{y_1+y_2+y_3}{3}\right)$.

15 3D Geometry

Until now, we've mostly only looked at geometry in the Euclidean plane. Today, we'll explore geometry in three dimensions, which requires more visual intuition.

§15.1 3D Shapes

There are many shapes that can be drawn in 3D space. The ones that we'll focus on, as well as the most frequently appearing ones on contests, are *planes*, *prisms*, *polyhedra*, *spheres*, *cones*, and *cylinders*.

§15.1.1 3D Coordinates

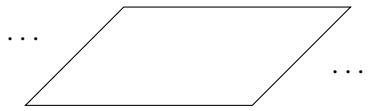
Before we begin, we first introduce a coordinate system for 3D shapes – which is quite similar to our 2D coordinate system.

Definition 15.1. **3D coordinate space** is the set of all points (x, y, z) for real numbers x, y, z. The number x represents the displacement from the yz-plane, while y represents the displacement from the xz-plane and z is the displacement from the xy-plane.

You can think of this as taking a point in the familiar xy-plane then moving it so it levitates above or below with a certain displacement z away from the plane.

§15.1.2 Planes

Definition 15.2. A **plane** is a flat, 2D surface in 3D space.



> **Example 15.3.** Remember that it takes 2 points in 2D (or 3D) space to determine a line. How many points does it take to determine a plane?

Solution. It takes **3** points. Note that a plane is just a collection of lines stacked onto each other. We can choose such a line (2 points determine a line), and then another point that the plane must contain. As planes must be flat surfaces, there is only one such plane that can contain the point and the line. ■

> *Remark.* These three points must not be collinear; otherwise, they simply form a line, which could be contained by infinitely many planes.

Exercise 15.4. Two non-parallel lines intersect at a point. How do two intersecting planes intersect? Must two arbitrary planes intersect?

Exercise 15.5. Let lines s, t intersect at P. Must s and t both be contained in some plane?

§15.1.3 Prisms and Polyhedra

Definition 15.6. A **prism** is a 3D solid figure with two congruent polygonal bases, either of which can be translated to the other (they are at the "top" and "bottom"). The faces which are not bases are called **sides**. All sides have equal height, and the edges exlusive to side faces are perpendicular to the edges which form the bases.

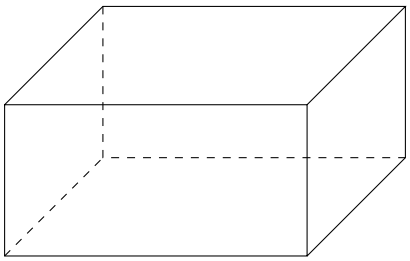
You can think of a prism as taking a polygon (which will be the bases), then stacking it on top of itself repeatedly until it is no longer flat and is three-dimensional.

Definition 15.7. A **right** prism is a prism where the sides are perpendicular to both bases.

Unless otherwise noted, prisms are generally assumed to be right.

Definition 15.8. A **rectangular** prism is a prism with a rectangular base.

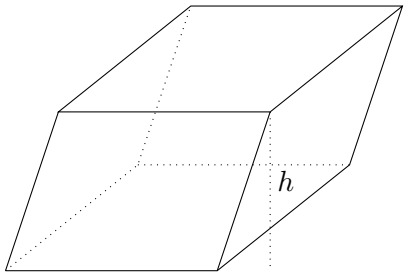
Note that a rectangular prism does not necessarily have to be right, though in competition math rectangular prisms will be assumed to be right unless otherwise specified.



Example 15.9. The volume of a right rectangular prism is lwh, where l is the length, w is the width, and h the height of the rectangular prism.

Definition 15.10. A **regular** prism is a prism with a regular polygon as a base.

Definition 15.11. A **parallelepiped** is a prism where *all* faces are parallelograms.



Note that the two bases are the side facing us and the side opposite of that.

Exercise 15.12. Describe to the best of your ability the cross-section of a parallelepiped parallel to one of its faces.

We next talk about polyhedra.

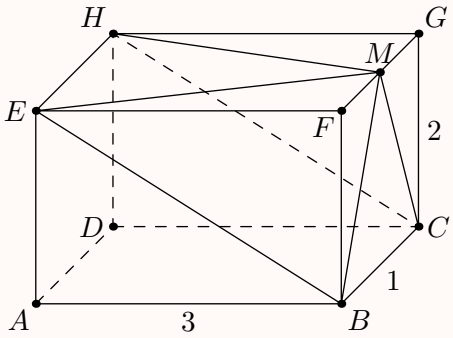
Definition 15.13. A **polyhedron** is a 3D shape with all faces as polygons.

Two types of polyhedra are most of interest: pyramids and regular polyhedra.

Definition 15.14. A **pyramid** is a polyhedron formed by connecting all the vertices of a polygon to a point not in the same plane as the polygon. This point is known as the **apex**. Like with prisms, a pyramid is **regular** if it has a regular polygon as a base. A **right pyramid** is a regular pyramid whose apex is directly above the center of the base.

The volume of a pyramid is $\frac{1}{3}bh$, where b is the area of the base and h is the height of the pyramid — the distance between the base and the top vertex.

Example 15.15 (AMC 10). In the rectangular prism shown, $AB = 3$, $BC = 1$, and $CG = 2$. Point M is the midpoint of $\overline{FG}$. What is the volume of the rectangular pyramid with base $BCHE$ and apex M?



Solution. Although it's quite easy to find the base of said pyramid, we would need to coordinate bash to find the height of the pyramid. As coordinate bashing was the topic of the previous section, we leave this as an exercise for the reader.

Another method to find the volume is quite similar to complementary counting in combinatorics. Note that plane $BCHE$ splits prism $ABCDEFGH$ up into two equal halves. As the volume of $ABCDEFGH$ is 6, the half that contains pyramid $MBCHE$ must have volume 3.

The two regions in this half that are not contained in $MBCHE$ are triangular pyramids $BMFE$ and $CMGH$. Use the formula stated above to show that the volumes of $BMFE$ and $CMGH$ are both $\frac{3 \cdot 2 \cdot \frac{1}{2}}{3} = 1$. Thus, the volume of $MBCHE$ is 2. ■

Remark. Another name for a triangular pyramid is a **tetrahedron**. Some other -hedra to know the names of:

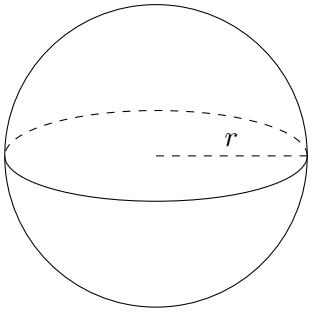
Polygon name	Number of faces
tetrahedron	4 faces
hexahedron	6 faces
octahedron	8 faces
dodecahedron	12 faces
icosahedron	20 faces

These polyhedra are the only polyhedra that can be regular. (The regular hexahedron is the cube.) Note that the name depends on the number of faces.

Exercise 15.16 (AMC 10). The centers of the faces of the right rectangular prism with dimensions $3 \times 4 \times 5$ below are joined to create an octahedron. What is the volume of this octahedron?

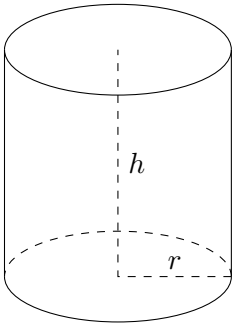
§15.1.4 Spheres, Cones, and Cylinders

Definition 15.17. A **sphere** is the set of points in 3D space equidistant (with distance r) from a point O. We call O the **center** and r the **radius**.

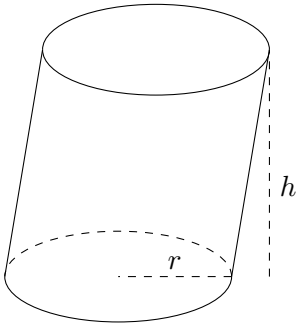


The volume of a sphere is $V = \dfrac{4\pi r^3}{3}$, as you may remember.

Definition 15.18. A **cylinder** is the resulting solid after rotating a parallelogram about one of its edges. The cylinder is **right** if this parallelogram is a rectangle.



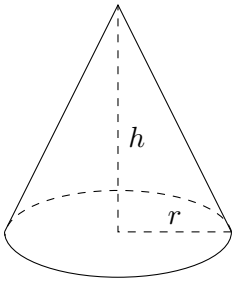
A right cylinder.



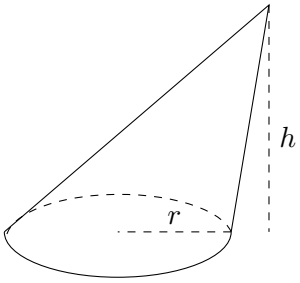
An oblique cylinder.

Definition 15.19. A **cone** is the set of points on the lines from a point P to a circle ω *NOT* on the same plane as the point. ω is the base and P is a cone.

Let O be the center of ω. The cone is **right** of $OP \perp OX$ for all X on ω.



A right cone.



An oblique cone.

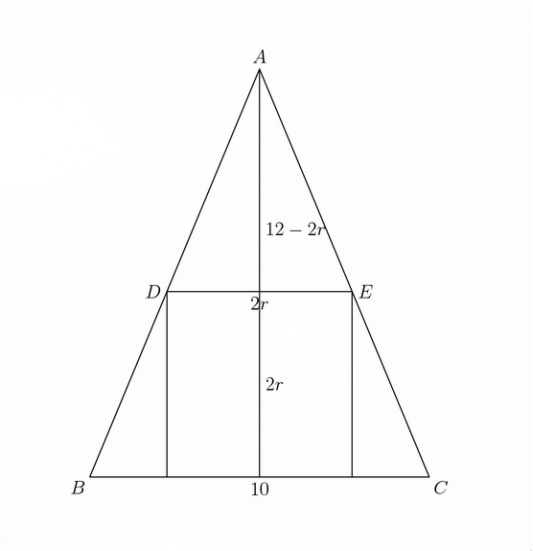
Like in prisms and pyramids, cylinders and cones are assumed to be right unless otherwise stated. We can imagine cylinders as "circular prisms" and cones as "circular pyramids".

Therefore, the volume of a cylinder is just bh. But we know $b = \pi r^2$ where r is the radius. Thus, we have that the volume is $\pi r^2 h$.

The volume of a cone, similarly, is $\dfrac{\pi r^2 h}{3}$ from similar reasoning with cones.

Example 15.20 (AMC 10)**.** A right circular cylinder with its diameter equal to its height is inscribed in a right circular cone. The cone has diameter 10 and altitude 12, and the axes of the cylinder and cone coincide. Find the radius of the cylinder.

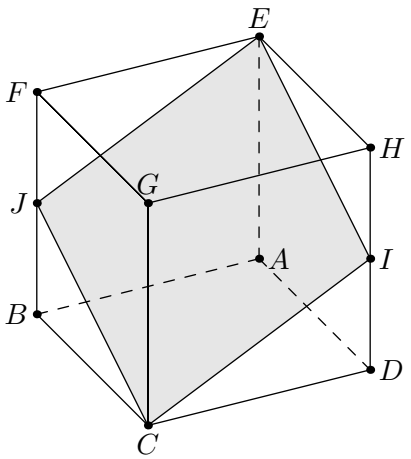
Solution. The key strategy for this problem is taking the cross-section perpendicular to a diameter, as shown below. Let the radius of the cone be r and the midpoint of BC be M and the midpoint of DE be N. We then have the following diagram.



We now use similar triangles. We know from AA similarity that $\triangle AMB \sim \triangle AND$. Therefore, $\dfrac{5}{12} = \dfrac{r}{12-2r}$. This just turns into algebra, which we leave as an exercise to the reader. Our final answer is $\dfrac{30}{11}$. ■

The key concept here was taking 2D cross-sections. In fact, most such 3D problems can be solved by taking clever 2D cross-sections, then using our knowledge of 2D geometry.

Exercise 15.21 (AMC 8). In the cube $ABCDEFGH$ with opposite vertices C and E, J and I are the midpoints of segments $\overline{FB}$ and $\overline{HD}$, respectively. Let R be the ratio of the area of the cross-section $EJCI$ to the area of one of the faces of the cube. What is R^2?

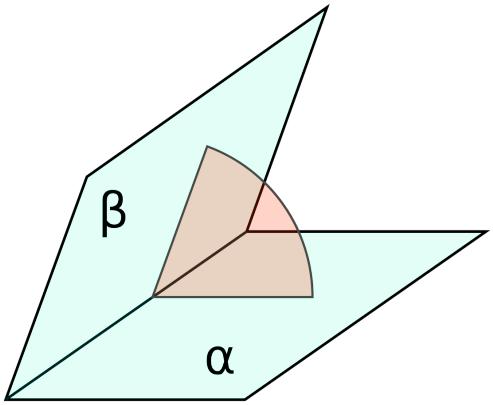


Exercise 15.22 (AMC 12). A sphere with center O has radius 6. A triangle with sides of length $15, 15$, and 24 is situated in space so that each of its sides is tangent to the sphere. What is the distance between O and the plane determined by the triangle?

§15.1.5 Dihedral Angles

Definition 15.23. A **dihedral angle** is the angle between two intersecting planes. Two planes are **perpendicular** if their dihedral angle is 90°.

In the diagram below, α and β are planes and the angle between them is the dihedral angle.



When we take cross-sections, we can think of dihedral angles as regular angles in 2D geometry.

Exercise 15.24 (AMC 12). Triangle PAB and square $ABCD$ are in perpendicular planes. Given that $PA = 3$, $PB = 4$, and $AB = 5$, what is PD?

Exercise 15.25 (AIME). A right prism with height h has bases that are regular hexagons with sides of length 12. A vertex A of the prism and its three adjacent vertices are the vertices of a triangular pyramid. The dihedral angle (the angle between the two planes) formed by the face of the pyramid that lies in a base of the prism and the face of the pyramid that does not contain A measures 60 degrees. Find h^2.

§15.2 Volume and Surface Area

Definition 15.26. The **lateral surface area** of an object is the area of all the sides excluding the area of its base and top.

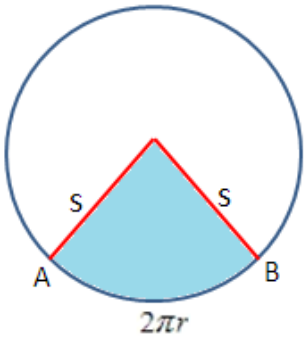
Proposition 15.27. *The volume of an object is proportional to its lengths cubed, while the surface area of an object is proportional to its length squared.*

As a result, the volume ratio between two similar objects is equal to the cube of the ratio of their respective lengths, and the surface area ratio between two similar objects is equal to the square of the ratio of their respective lengths.

Example 15.28. What is the lateral surface area of a cone with radius r and slant height s?

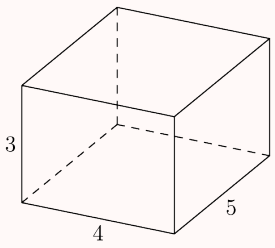
Solution. The **slant height** of a cone is the distance between the apex and a point on the circumference of the circular base.

Observe that we may unwrap the cone into a 2-D shape. More specifically, it unwraps into a sector of a larger circle with radius s. The arc length of the sector is the circumference of the base of the cone: $2\pi r$.

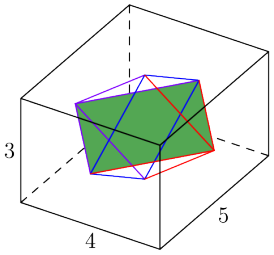


Hence, the sector is $\frac{2\pi r}{2\pi s}$ of the whole circle, meaning that the area of the sector, and thus the lateral surface area of the cone, is $\pi s^2 \cdot \frac{2\pi r}{2\pi s} = \pi rs$. ■

Example 15.29 (AMC 10)**.** The centers of the faces of the right rectangular prism shown below are joined to create an octahedron, What is the volume of the octahedron?



Solution. Note that the octahedron is two pyramids attached at the base. As a result, it suffices to find the volume of one such pyramid and multiply by two. The base of the pyramid is highlighted in green.



Observe that the shaded figure is actually a rhombus, and its diagonals are parallel to the sides of the prism and hence perpendicular to each other. Thus, the area of the shaded rhombus is

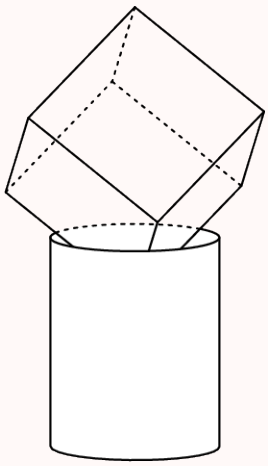
$$\frac{1}{2} \cdot 4 \cdot 5 = 10.$$

Finally, the height of one of the pyramids is half of the height of the octahedron, which is the height of the prism: 3. Hence, each prism has volume

$$\frac{1}{3} \cdot 10 \cdot \frac{3}{2} = 5,$$

meaning the volume of the final octahedron is $2 \cdot 5 = 10$. ■

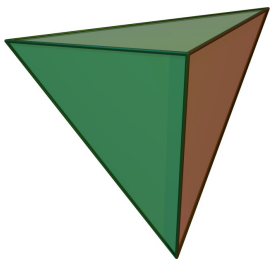
Example 15.30 (AIME). A cylindrical barrel with radius 4 feet and height 10 feet is full of water. A solid cube with side length 8 feet is set into the barrel so that the diagonal of the cube is vertical. The volume of water thus displaced is v cubic feet. Find v^2.



Solution. The volume of water displaced is the volume taken up by the cube in the cylinder. The portion of the cube in the water is a right triangular pyramid, as it is the corner of the cube.

Note that the condition, "the diagonal of the cube is vertical" is important here. A direct corollary is that the line determined by the center of the cube and the center of the cylinder is the diagonal of the cube. (Convince yourself that this is true before continuing.)

As a result, the three legs of the tetrahedron are equal because of rotational symmetry. Hence, the desired tetrahedron has three isosceles right triangle faces and one equilateral triangle face, resembling something like below, where the three isosceles faces meet at pairwise right angles:



Let the legs of each of the isosceles right triangle faces have length x, and thus the other three edges have length $x\sqrt{2}$. With this knowledge, we are ready to tackle the computation. As usually helpful with 3D problems, we should consider cross-sections in order to convert this problem into a 2D problem. Namely, the cross-section between the cube and cylinder is the equilateral triangle face of our tetrahedron with length $x\sqrt{2}$!

Moreover, note that the circumcircle of this equilateral triangle is the base of the cylinder, which is a circle with radius 4. Hence, it suffices to find x such that the circumradius of the equilateral triangle with length $x\sqrt{2}$ is 4.

This is simple enough and can be done in several ways. We present two methods.

Method 1 (Triangle Centers): Observe that the length of the circumradius of an equilateral triangle is the distance from a vertex to the circumcenter. Recall that the centroid, orthocenter, and circumcenter of an equilateral triangle are the same point. Hence, by centroid ratios, the circumradius, R, is 2/3 of the altitude. Thus, we have

$$\frac{3}{2}R = (x\sqrt{2}) \cdot \frac{\sqrt{3}}{2},$$

Giving that when $R = 4$, $x = 2\sqrt{6}$.

Method 2 (Extended Law of Sines): Recall that by the extended law of Sines,

$$2R = \frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}$$

Hence, when $R = 4$ in an equilateral triangle, we have

$$8 = \frac{x\sqrt{2}}{\sin 60^\circ},$$

Solving for x gives $x = 2\sqrt{6}$, as well.

Of course, we are not finished! We must find the volume of the tetrahedron. However, this is quite simple, for since the three isosceles right triangle faces are pairwise perpendicular, then the volume is simply

$$v = \frac{1}{3} \cdot \left(\frac{1}{2}x^2\right) \cdot x = \frac{1}{6}x^3,$$

whence for $x = 2\sqrt{6}$, $v = 8\sqrt{6}$. Finally, we are left with $v^2 = 384$. ■

Exercise 15.31 (AMC 10). A pyramid with a square base is cut by a plane that is parallel to its base and is 2 units from the base. The surface area of the smaller pyramid that is cut from the top is half the surface area of the original pyramid. What is the altitude of the original pyramid?

Exercise 15.32 (AIME). Two congruent right circular cones each with base radius 3 and height 8 have axes of symmetry that intersect at right angles at a point in the interior of the cones a distance 3 from the base of each cone. Find the volume of the maximal sphere that can lie inside both cones.

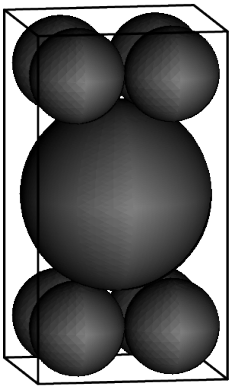
§15.3 Homework Problems

Problem 15.1. [3] A sphere with radius r has volume 36π. If a cone with radius r and height h has the same volume as the sphere, find h.

Problem 15.2. [4] Let $\mathcal{A}$ denote the region of points in space with a distance at most 1 unit away from a $3 \times 3 \times 3$ cube. If the volume of $\mathcal{A}$ can be represented as $a + \frac{b\pi}{c}$ where a, b, c are integers and b, c are relatively prime, find $a + b + c$.

Problem 15.3 (2007 AMC 12A)**.** [6] Corners are sliced off a unit cube so that the six faces each become regular octagons. If the total volume of the removed tetrahedra can be expressed in the form $\frac{a-b\sqrt{c}}{d}$, where c is square free and $\gcd(a, b, d) = 1$, then find $abcd$.

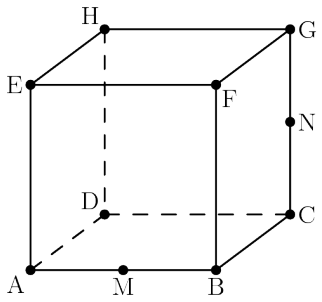
Problem 15.4 (2014 AMC 12A)**.** [6] A $4 \times 4 \times h$ rectangular box contains a sphere of radius 2 and eight smaller spheres of radius 1 (diagram below). The smaller spheres are each tangent to three sides of the box, and the larger sphere is tangent to each of the smaller spheres. If h can be expressed in the form $a + b\sqrt{c}$, find $a + b + c$.



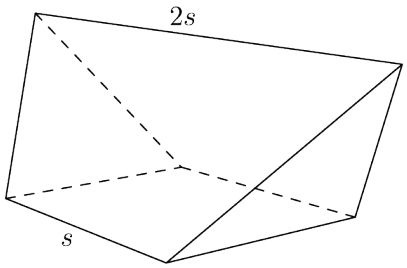
Problem 15.5. [6] Let $ABCD$ be a tetrahedron, and let planes ACD and BCD intersect at a 60° angle, and $\triangle BCD$ is an isosceles right triangle with $\angle BCD = 90^\circ$. Let F be the foot of the perpendicular from A to $\overline{BD}$. Let E be the point on DE such that $BC||EF$ and both lines are coplanar. If $AD = 5$ and $DF = 3$, find AE^2.

Problem 15.6 (2005 HMMT)**.** [8] A cube with side length 2 is inscribed in a sphere. A second cube, with faces parallel to the first, is inscribed between the sphere and one face of the first cube. THe side length of the smaller cube can be expressed in the form m/n where m, n are relatively prime. Find $m + n$.

Problem 15.7 (2012 AIME I)**.** [10] Cube $ABCDEFGH$, labeled as shown below, has edge length 1 and is cut by a plane passing through vertex D and the midpoints M and N of $\overline{AB}$ and $\overline{CG}$ respectively. The plane divides the cube into two solids. The volume of the larger of the two solids can be written in the form $\frac{p}{q}$, where p and q are relatively prime positive integers. Find $p + q$.



Problem 15.8 (1983 AIME)**.** [7] The solid shown has a square base of side length s. The upper edge is parallel to the base and has length $2s$. All other edges have length s. Given that $s = 6\sqrt{2}$, what is the volume of the solid?



Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

16 Basics & Arithmetic Functions

§16.1 Basics

Number theory is the study of integers, and is often considered one of the most beautiful subjects in math because of its depth. In this handout, we'll introduce the most basic concepts in number theory and begin exploring arithmetic functions, which will be very useful later this week.

Definition 16.1. A positive integer p is **prime** if it has only 2 distinct positive divisors, 1 and itself.

Definition 16.2. A positive integer is **composite** if and only if it is not prime and not equal to 1.

You can think of a composite number as being built out of more than one (not necessarily distinct) prime factors.

Definition 16.3. We say that n is a **multiple** of m if there exists an integer a such that $n = am$.

Definition 16.4. We say that m is a divisor of n if n is a multiple of m; that is, there exists an integer a such that $n = am$. We write $m \mid n$ if m divides n and $m \nmid n$ if m does not divide n.

Definition 16.5. We say that n and m are **relatively prime** if they share no common factors besides 1. That is, $\gcd(m, n) = 1$.

Note that with respect to the idea of division, primes are the "building blocks" of integers; we can decompose any integer into a product of powers of primes. This is intuitive because primes are the only integers that cannot be further divided, in the sense that they do not have factors distinct from themselves.

Exercise. Prove that if a prime p divides ab where a and b are integers, then p divides a or p divides b.

Example 16.6. Show that 37 is prime.

Solution. A prime number has no other divisors other than 1 and itself. So, let us check all the integers between 1 and p, exclusive. We can see that 37 is not even, so 2 does not divide it. We can also check that 3 does not divide 37 through a quick check. 4 clearly does not divide 37 since, again, 37 is not even...

This is taking quite a while. In fact, using this approach, we would have to check the divisibility of 35 integers! Let us find some optimizations for checking if a number is prime.

First of all, note that if an integer k divides p, then $\frac{p}{k}$ also divides p. That is, factors come in pairs. Moreover, if $k < \sqrt{p}$, then

$$\frac{p}{k} > \frac{p}{\sqrt{p}} = \sqrt{p},$$

and vice versa. This means that we only have to test the first $\lfloor \sqrt{p} \rfloor$ positive integers for divisibility. If we cannot find such a divisor, the number is prime. The number cannot only have factors greater than $\sqrt{p}$, since a factor greater than $\sqrt{p}$ would have a factor pair less than $\sqrt{p}$.

This significantly reduces work, as now we only have to check for divisibility by $2, 3, 4, 5, 6$, which we can quickly do. However, what if the number was larger? We can still optimize this process further. Notice how if, say $6 \mid n$, then $2 \mid n$, and $3 \mid n$. If $2 \nmid n$, then 6 could not possibly divide n. This leads us to see that we only have to check for divisibility of the factors' "building blocks". That is, we only have to check for divisibility of prime factors. Thus, we reduce the list of factors $2, 3, 4, 5, 6$ to $2, 3, 5$, which we can very easily check to determine that 37 is indeed prime. ■

By the same argument we used here, in general for an integer n, we only need to test primes less than or equal to $\sqrt{n}$ to see if n is prime.

Taking the idea that primes are building blocks further, we can form the following definition:

Definition 16.7. A **prime factorization** of an integer n is a representation of n as products of powers of primes:

$$n = {p_1}^{k_1} {p_2}^{k_2} \dots {p_m}^{k_m}.$$

Theorem 16.8 (Fundamental Theorem of Arithmetic). *Every integer has a unique prime factorization up to the ordering of the prime powers.*

This theorem is what makes prime factorizations so important; they are unique representations of integers that give us more information on their divisors.

Example 16.9. Prime factorize 60.

Solution. Begin by checking for prime factors starting from 2 and going up. When you find a prime factor, divide by the prime and repeat to find the highest power of the prime dividing the integer. In this case, we first test 2 and see that 2 indeed divides 60. Now we write down 2 and test $60/2 = 30$. We again see that 2 divides 30, so now write down another 2 and test $30/2 = 15$. 2 does not divide 15, so we move on to 3, which divides 15. We write down 3. Now we are left with 5, which is a prime. Checking the prime factors we've written down, we see the prime factorization is $2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$. ■

Example 16.10. Prime factorize $21^3 - 10^3$.

Solution. We could calculate $21^3 - 10^3$ and prime factorize that, but there is no need to. We quickly see that the expression is a difference of cubes. Since we can factor a difference of cubes, and our goal is to completely factor the expression, this helps quite a lot. Applying difference of cubes, we have

$$\begin{aligned} 21^3 - 10^3 &= (21 - 10)(21^2 + 21 \cdot 10 + 10^2) \\ &= 11 \cdot (441 + 210 + 100) \\ &= 11 \cdot 751 \end{aligned}$$

We see that 11 is clearly prime, and we can check that 751 is prime by checking divisibility of all the primes from 2 to $\lfloor\sqrt{751}\rfloor = 27$, inclusive. Thus, our answer is $11 \cdot 751$. ■

Remark. The format of the expression in the problem made it pretty obvious that we were dealing with a difference of cubes. However, this may not always be the case. For instance, it maybe a little more difficult to see that 9919 is a difference of squares $(100^2 - 9^2)$. The factorization may even be a little more complicated. For example,

$$\begin{aligned} 100064 &= 10^4 + 4 \cdot 2^4 \\ &= (10^2 - 2 \cdot 10 \cdot 2 + 2^2)(10^2 + 2 \cdot 10 \cdot 2 + 2^2) \end{aligned}$$

is factorable by Sophie-Germain's Identity. When coming across a special-looking number to factor, keep an eye out for these common factorizations!

Example 16.11 (1998 AHSME)**.** If 1998 is written as a product of two positive integers whose difference is as small as possible, then the difference is

(A) 8 (B) 15 (C) 17 (D) 47 (E) 93

Solution. We could find all the factors of 1998, then find the factor pair with the smallest difference, but it is a bit easier to prime factorize 1998, then separate the factors into two groups of close products.

After some work similar to example 16.9, we can see that

$$1998 = 2 \cdot 3^3 \cdot 37.$$

We note that 37 is noticeably bigger than the other factors, so we put that aside and calculate $2 \cdot 3^3 = 54$. This gives a difference of $54 - 37 = 17$.

We might wonder if it is possible for the factors to be even closer together. To answer this, note that one of the two factors must have 37 as a factor. Say it is $37k$, where k is an integer greater than 2. The other factor in the pair is $\frac{1998}{37k}$. Now, note that $k \geq 2$ implies that $37k \geq 74$, so we must have

$$\frac{1998}{37k} \leq \frac{1998}{74} = 27.$$

This difference is greater than 17, so (C) 17 is our answer. ■

Example 16.12. Find the largest perfect square that divides 9!.

Solution. A perfect square is a number that can be written in the form k^2 for some positive integer k. If the prime factorization of k is

$${p_1}^{k_1} {p_2}^{k_2} \dots {p_m}^{k_m},$$

then the prime factorization of k^2 is

$$\left({p_1}^{k_1} {p_2}^{k_2} \dots {p_m}^{k_m}\right)^2$$
$${p_1}^{2k_1} {p_2}^{2k_2} \dots {p_m}^{2k_m}.$$

In other words, a number is a perfect square if and only if the exponents in its prime factorization are even.

We first prime factorize 9!:

$$\begin{aligned} 9! &= 9 \cdots 2 \cdot 1 \\ &= (3^2) \cdot (2^3) \cdots (2^2) \cdot 3 \cdot 2 \cdot 1 \\ &= 2^7 \cdot 3^4 \cdot 5^1 \cdot 7^1. \end{aligned}$$

We wish to find that largest perfect square that divides 9!, so we will take the largest power with an even exponent of each prime factor. Doing so gives an answer of

$$2^6 \cdot 3^4 \cdot 5^0 \cdot 7^0 = 5184.$$

■

Example 16.13 (1983 AIME). What is the largest 2-digit prime factor of the integer $n = \binom{200}{100}$?

Solution. It is not clear what the prime factors of a binomial coefficient are; it is certainly easier to find the prime factors of a factorial. Rewriting $\binom{200}{100}$ with factorials gives

$$\binom{200}{100} = \frac{200!}{100! \cdot 100!}.$$

There are two 100!'s in the denominator, which seems pretty nice. Assume the highest power of a prime p dividing 100! is p^k for some integer k. Then we know that we have a total of $2k$ factors dividing the denominator, so we need at least $2k+1$ factors of p in 200!.

The most logical first case to consider is when $k = 1$, since we want our prime to be as big as possible. Note that this implies that $p \geq 53$ (why?). Then we know

$$p^3 \mid 200!.$$

Since 200! is the product of every integer from 1 to 200 inclusive, if $p^3 \mid 200!$, p must divide at least 3 of these integers; we can't have an integer with repeated factors of p since $p \geq 53$.

A positive integer is divisible by p if it can be written in the form pk for some integer k. The lowest positive values pk can take are $p, 2p, 3p$. Therefore, we must have $3p \leq 200$ in order for p to appear 3 times in the product of the integers from 1 to 200.

The largest prime p that satisfies $3p \leq 200$ is 61 by trial and error. We can indeed check that $61^3 \mid 200!$ since

$$\begin{aligned} 200! &= 200 \cdot 199 \cdots 184 \cdot 183 \cdot 182 \cdots 127 \cdot 126 \cdot 125 \cdots 61 \cdots 2 \cdot 1 \\ &= 200 \cdot 199 \cdots 184 \cdot (3 \cdot 61) \cdot 182 \cdots 127 \cdot (2 \cdot 61) \cdot 125 \cdots (1 \cdot 61) \cdots 2 \cdot 1 \\ &= 61^3 \cdot (\cdots) \end{aligned}$$

We can also check that 61 divides 100! once, which implies that 61^2 divides $100! \cdot 100!$ once. Thus, $\binom{200}{100}$ is divisible by $\frac{61^3}{61^2} = 61$. ■

Exercise. Prime factorize $2^{16} - 1$.

Exercise (2001 AMC 12). Four positive integers a, b, c, and d have a product of 8! and satisfy:

$$ab + a + b = 524$$
$$bc + b + c = 146$$
$$cd + c + d = 104$$

What is $a - d$?

§16.1.1 Number and Sum of Divisors

Definition 16.14. The **number of divisors function**, denoted $\tau(n)$, is the number of positive integer divisors of n, or

$$\sum_{d|n} 1$$

Proposition 16.15. *Assume n has prime factorization*

$$p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}.$$

Then

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_m + 1).$$

Proof. Consider the prime factorization any divisor of n. It can only have primes in the prime factorization of n, and they must be to a power less than or equal to the power of that prime in the factorization of n.

For example, assume $d \mid n$ and that the maximum power of p_1 dividing d is ${p_1}^r$. Then we know that $0 \le r \le k_1$, so there are $k_1 + 1$ possibilities for r.

The same logic holds for any prime p_i, so let's consider constructing a divisor of n. We first choose what power of p_1 it has from the range 0 to k_1, inclusive, then choose what power of p_2 it has from the range $0 to k_2$ inclusive, and so on. For each prime p_i there are $k_i + 1$ possibilities, so we get

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_m + 1).$$

■

Example 16.16. Find $\tau(360)$.

Solution. Since $360 = 2^3 \cdot 3^2 \cdot 5^1 \cdot$, we get $\sigma(360) = (3 + 1)(2 + 1)(1 + 1) = 24$. ■

Example 16.17 (2005 AMC 10A). How many positive cubes divide $3! \cdot 5! \cdot 7!$?

Solution. $\sigma(3! \cdot 5! \cdot 7!)$ does not seem like much help, as the problem asks for factors that are cubes. What can we do now?

First, let us find the prime factorization of the number. We have

$$3! \cdot 5! \cdot 7! = 3 \cdot 2 \cdot 5 \cdot 4 \cdots = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

Now that we have the prime factorization, we should consider how to count the number of factors that are cubes. We take inspiration from the derivation of the formula for the number of divisors function.

A perfect cube is an integer that can be written as k^3 for some positive integer k. This means that the exponents in the prime factorization of a perfect cube are divisible by 3. Given this, how many possibilities are there for the power of 2 in the prime factorization of a cubic factor?

We can either choose $2^0, 2^3$, or 2^6, since the power of 2 in the prime factorization of $3! \cdot 5! \cdot 7!$ is 2^8. What about for 3? The power of 3 in the prime factorization of of $3! \cdot 5! \cdot 7!$ is 3^4, so we have 2 choices, 3^0 and 3^3. Similarly, we have 1 choice for 5 and 1 choice for 7.

Our answer is the product of the number of choices for each prime factor, which is

$$3 \cdot 2 \cdot 1 \cdot 1 = 6.$$ ■

Example 16.18 (1990 AIME). Let n be the smallest positive integer that is a multiple of 75 and has exactly 75 positive integral divisors, including 1 and itself. Find $\frac{n}{75}$.

Solution. Let us first ignore the multiple of 75 condition. We prime factorize 75 as $3 \cdot 5^2$. Since we wish for $n = p_0^{e_0} p_1^{e_1} \cdots$ to have 75 factors, we need

$$\begin{aligned} \sigma(n) &= (e_0 + 1)(e_1 + 1) \cdots \\ &= 75 \\ &= 3 \cdot 5^2. \end{aligned}$$

Of course, it is possible to have something like $k = 2^{74}$ so that $\sigma(k) = 75$, but this number is incredibly large. In order to make n small, we would want to distribute the factors more evenly.

We should also note that the exponents should be arranged in decreasing order. For example, $n = 2^4 \cdot 3^4 \cdot 5^2$ is better than $n = 2^2 \cdot 3^4 \cdot 5^4$ since arranging the exponents in decreasing order minimizes n. Similarly, $n = 2^0 \cdot 3^2 \cdot 5^1$ is greater than $n = 2^2 \cdot 3^1 \cdot 5^0$, so we want to choose the minimal exponent bases, so long as our resulting n satisfies the problem condition that $75 \mid n$.

With these facts, we consider possible distributions. Splitting $75 = 3 \cdot 5 \cdot 5$ gives $n = 2^{5-1} \cdot 3^{5-1} \cdot 5^{3-1} = 2^4 \cdot 3^4 \cdot 5^2$. This is, in fact, the least we can do. If you are not convinced, you can try things like $75 = 5 \cdot 15$, but you will see that exponential growth just inflates numbers too quickly. Note that there may be some instances in which the prime bases grow faster; that is, it is beneficial to split 75 into fewer factors. However, this is not one of them.

We note that $n = 2^4 \cdot 3^4 \cdot 5^2$ is luckily divisible by $75 = 3 \cdot 5^2$, so our answer is $\frac{n}{75} = \frac{2^4 \cdot 3^4 \cdot 5^2}{3 \cdot 5^2} = 432$. ■

Remark. If 75 did not divide n, we might have to redistribute the factors to satisfy the constraint. This is one of those exceptions where it is possible for the best solution to not have decreasing exponents.

Here's a final example that demonstrates how knowing small values of $\tau(n)$ can give us information on what n looks like:

Example 16.19 (2019 AIME I). Let $\tau(n)$ denote the number of positive integer divisors of n. Find the sum of the six least positive integers n that are solutions to $\tau(n) + \tau(n+1) = 7$.

Solution. The first thing you should notice is that $\tau(n)$ and $\tau(n+1)$ are integers, so they could be $(1,6),(2,5),(3,4)$ and permutations. However, we can actually get rid of the first case, since $\tau(n) \geq 2$ (always have 1 and n as a divisor). Thus, we have four cases:

- **Case 1a:** $\tau(n) = 2$, $\tau(n+1) = 5$. If $\tau(n) = 2$, then it must be prime. What about $\tau(n+1) = 5$? Well, the product of the exponents for each prime incremented by one is the formula for τ, so that means that the exponents incremented by one must be of the form $(5, 1, 1 \cdots 1)$ in some order of primes. Decreasing by one to get the exponent, that gives $(4, 0, \cdots 0)$, so that means $n+1$ must be some perfect fourth power of a prime number! Let $n = p$ for some prime p and $n + 1 = q^4$ for some prime q. We then have

  $$n + 1 = q^4 \implies p + 1 = q^4 \implies p = q^4 - 1 = (q^2+1)(q^2-1) = (q^2+1)(q+1)(q-1)$$

  Since p is prime, we must have two of the factors be 1 and the other be p. However, $q^2 + 1 \geq q + 1 > q - 1$, so the smallest two numbers can't both be one since they are always different. Thus, we have 0 solutions in this case.

- **Case 1b:** $\tau(n) = 5$, $\tau(n+1) = 2$. We know from case 1 that this means $n = q^4$ for some prime q and $n + 1 = p$ for some prime p. This means

  $$n + 1 = p \implies q^4 + 1 = p$$

  If $q = 2$, we get $p = 17$, which works (so $n = 16$). However, if q is odd, then p must be even, meaning $p = 2$. This corresponds to $q = 1$, contradiction of q is prime, so $n = 16$ is the only solution in this case.

- **Case 2a:** $\tau(n) = 3$, $\tau(n+1) = 4$. What does $\tau(n) = 3$ mean? Well, let's go through a similar process for when we analyzed $\tau(n) = 5$. Since 3 is prime, the set of all exponents of primes incremented by 1 is $(3, 1, \cdots, 1)$, so the exponents must be $(2, 0, \cdots, 0)$. Thus, n must be some prime squared: let $n = p^2$ for some prime p.

  What does $\tau(n+1) = 4$ mean? Performing a similar process, we can see that this means the set of exponents incremented by one are either $(4, 1, \cdots, 1)$ or $(2, 2, 1 \cdots, 1)$, so the set of exponents could be $(3, 0, \cdots, 0)$ or $(1, 1, 0, \cdots, 0)$. Thus, $n+1$ is either some prime cubed, or the product of two different primes. Suppose the latter option for now, and let $n + 1 = q^3$ for some prime q. We then have

  $$n + 1 = q^3 \implies p^2 + 1 = q^3 \implies p^2 = (q-1)(q^2+q+1)$$

  Note that $q^2 + q + 1 > q - 1$, so we must have that $q - 1 = 1$ and $q^2 + q + 1 = p^2$, giving $q = 2 \implies p^2 = 7$, a contradiction. This means we have no solution for when $n + 1$ is a perfect cube of a prime. Suppose now that $n = qr$ for some primes q and r. We then have

  $$n + 1 = qr \implies p^2 + 1 = qr$$

  If $p = 2$, we have no solutions for q and r that give both of them are prime, so henceforth assume p is odd. Then, qr is even, meaning either q or r is equal to 2. If both are equal to 2, that gives $p^2 = 3$, contradiction, so at most one can be equal to 2. WLOG, let $r = 2$. We have

  $$p^2 + 1 = 2q$$

  At this point, we can just manually find some small values of p and q. It turns out that we have $(p, q) = (3, 5), (5, 13), (11, 61), (19, 181)$ are some of the smallest solutions, corresponding to $n = 9, 25, 121, 361$.

- **Case 2b:** $\tau(n) = 4$, $\tau(n+1) = 3$. For now, assume n is a perfect cube of a prime, or $n = p^3$ for some prime p and $n + 1 = q^2$ for some prime q. This gives

$$p^3 + 1 = q^2$$

If $p = 2$, we have $q = 3$, a valid solution, so $n = 8$ works. Otherwise, p is odd, meaning q even or $q = 2$. This yields a contradiction, since that means $p^3 = 3$, so there are no other solutions when n is of the form p^3.

Now suppose $n = pq$ for some primes p and q, and $n + 1 = r^2$ for some prime r. Then we have

$$pq + 1 = r^2 \implies pq = (r+1)(r-1)$$

If both p and q are odd, then r is even, meaning $r = 2$. This can be seen to give no solutions, so WLOG $q = 2$, meaning $2p = (r+1)(r-1)$. Since r is odd, $r+1$ and $r-1$ are both even, or $(r+1)(r-1) = 2p$ is divisible by 4. The only way for this to happen is for $p = 2$, but this gives an invalid solution for r, so there are no solutions in this case.

In summary, our six smallest solutions for n are $8, 9, 16, 25, 121, 361$, so our answer is 540. ■

Make sure to understand this! It is extremely important to be able to figure out what form n is in when you know $\tau(n)$. Also, another takeaway should be that analyzing parity, or whether or not it is even or odd, is extremely useful when dealing with primes since the only even prime is 2.

Definition 16.20. The **sum of divisors function**, denoted $\sigma(n)$, is the sum of all positive integers dividing n, or

$$\sum_{d|n} d$$

Proposition 16.21. *Assume n has prime factorization*

$$p_1{}^{k_1} p_2{}^{k_2} \dots p_m{}^{k_m}.$$

Then

$$\sigma(n) = \prod_{j=1}^{m} \sum_{i=0}^{k_j} p^i = (1 + p_1 + \dots + p_1{}^{k_1})(1 + p_2 + \dots + p_2{}^{k_2}) \dots (1 + p_m + \dots + p_m{}^{k_m}).$$

Example 16.22. Find $\sigma(360)$.

Solution. Since $360 = 2^3 \cdot 3^2 \cdot 5^1$, we get that the sum of the divisors is

$$\sigma(360) = (1 + 2 + 4 + 8)(1 + 3 + 9)(1 + 5) = 15 \cdot 13 \cdot 6 = 1170.$$

■

Example 16.23. Find the sum of the even factors of 360.

Solution. An even factor must have a power of 2 greater than 0 in its prime factorization. This leaves a lot of cases though, so we will instead calculate the sum of the odd factors, then subtract that from the sum of all the factors.

So, how do we calculate the sum of the odd factors? First, note that since 2 does not divide an odd factor, the factors of 2 are irrelevant. That is, if an odd factor is a factor of $2n$ for some integer n, it is also a factor of n. We can also see this through prime factorization. Thus, the sum of all the odd factors of 360 is equal to $\sigma\left(\frac{360}{2^k}\right)$, where k is the exponent of 2 in the prime factorization of 360. By prime factorizing, we see that $360 = 2^3 \cdot 3^2 \cdot 5$, so $\frac{360}{2^k} = 45$. We can now compute $\sigma(45) = (1+3+9)(1+5) = 78$.

Calculating the sum of the divisors of 360 is straightforward; it is just $\sigma(360) = 1170$.

Thus, the sum of the even divisors of 360 is $1170 - 78 = 1092$. ■

Exercise (Brilliant). Find the number of odd (positive) divisors of 7!

Exercise (2017 AMC 12B). The number $21! = 51,090,942,171,709,440,000$ has over $60,000$ positive integer divisors. One of them is chosen at random. What is the probability that it is odd?

Exercise. Prove Proposition 16.21. **Hint:** Expand the product given and see what you get.

§16.2 Euler Totient Function

Definition 16.24. The **Euler totient function**, denoted $\phi(n)$, is the number of integers from 1 to n, inclusive, that are relatively prime to n.

Proposition 16.25. *If n has prime factorization*

$$p_1{}^{k_1} p_2{}^{k_2} \dots p_m{}^{k_m}.$$

Then

$$\phi(n) = n \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

or similarly

$$\phi(n) = \prod_{i=1}^{m} \left(p_i^{k_i} - p_i^{k_i - 1}\right) = (p_1{}^{k_1} - p_1{}^{k_1-1})(p_2{}^{k_2} - p_2{}^{k_2-1}) \cdots (p_m{}^{k_m} - p_m{}^{k_m-1})$$

Proof. We will count the *fraction* of integers from 1 to n, inclusive, that are relatively prime to n. Then, we can simply multiply by n to get the number of integers. Note that the fraction of integers from 1 to n relatively prime to n is equivalent to the *probability* of randomly selecting an integer relatively prime to n.

In order for a number to be relatively prime to n, it must be relatively prime to each of its distinct prime factors, $p_1, p_2, \cdots, p_m$. Note that being relatively prime to one of these primes is independent of being relatively prime to any of the others, so the probability of a number being relatively prime to all of these primes is simply the product of the probabilities of being relatively prime to each prime separately.

Well, what's the probability a number is relatively prime to a prime p_i? Let's use complementary counting, and find the probability a number is divisible by p_i (convince yourself this

is equivalent to being not relatively prime to p_i). The number of integers from 1 to n that are divisible by n is simply $\frac{n}{p_i}$, since p_i divides n. This means the probability of randomly selecting one of these numbers is $\frac{\left(\frac{n}{p_i}\right)}{n} = \frac{1}{p_i}$. Since this is the complement, the probability of selecting an integer relatively prime to p_i in the range 1 through n is simply $1 - \frac{1}{p_i}$.

To get our final answer, we just need to multiply each of the probabilities and then multiply by n to get the number of integers:

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

which is exactly what we claimed. ■

Example 16.26. Find $\phi(60)$.

Solution. Since $60 = 2^2 \cdot 3^1 \cdot 5^1$, we get that the number of integers from 1 to 60, inclusive, that are relatively prime to 60 is $\phi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$. ■

Example 16.27. Find $\phi(p), \phi(p^2), \phi(p^k)$ for prime p and positive integer k.

Solution. The prime factorization of any prime number p is just p^1, so $\phi(p) = p \cdot (1 - \frac{1}{p}) = p - 1$. Similarly, p^2 is already prime factorized, so $\phi(p^2) = p^2 \cdots (1 - \frac{1}{p}) = p \cdot (p - 1)$. In general, $\phi(p^k) = p^k \cdot (1 - \frac{1}{p}) = p^{k-1} \cdot (p - 1)$. ■

Example 16.28. Let n be a positive integer. For how many integers $1 \leq k \leq n$ is $\frac{k}{n}$ simplified?

Solution. A fraction $\frac{a}{b}$ is simplified if a and b do not share any common factors. We can also state this as $\frac{a}{b}$ is simplified if $\gcd(a, b) = 1$, that is, a and b are relatively prime. But this is what the Euler totient function counts! Thus, we wish to find the number of integers k from 1 to n inclusive that are relatively prime to n, which is just $\phi(n)$. ■

Example 16.29 (1985 AIME). How many of the first 1000 positive integers can be expressed in the form

$$\lfloor 2x \rfloor + \lfloor 4x \rfloor + \lfloor 6x \rfloor + \lfloor 8x \rfloor,$$

where x is a real number, and $\lfloor z \rfloor$ denotes the greatest integer less than or equal to z?

Solution. If possible, we would like to minimize the expression inside the floor functions so that we can deal with fewer cases. That is, if we can take out an integer part of an expression inside the floor function, it will be easier to handle. We can do this by noting that $x = \lfloor x \rfloor + \{x\}$, since $\{x\}$, the fractional part of x, equals $x - \lfloor x \rfloor$ by definition. This will allow us to take out that $\lfloor x \rfloor$ out of the floor function, since we already know that it is an integer. Doing so gives

$$\begin{aligned}
\lfloor 2x \rfloor + \lfloor 4x \rfloor + \lfloor 6x \rfloor + \lfloor 8x \rfloor &= \lfloor 2(\lfloor x \rfloor + \{x\}) \rfloor + \cdots + \lfloor 8(\lfloor x \rfloor + \{x\}) \rfloor \\
&= (2\lfloor x \rfloor + \lfloor 2\{x\} \rfloor) + \cdots + (8\lfloor x \rfloor + \lfloor 8\{x\} \rfloor) \\
&= 20\lfloor x \rfloor + \lfloor 2\{x\} \rfloor + \lfloor 4\{x\} \rfloor + \lfloor 6\{x\} \rfloor + \lfloor 8\{x\} \rfloor.
\end{aligned}$$

Now, we think about how the expression changes as x changes. If the integer part of x changes by n, then the expression changes by $20n$ because of that first term.

The fractional part is a bit harder. We think about when $\lfloor k\{x\} \rfloor$ changes. From our knowledge of the floor function, we see that at $k\{x\} = 1, 2, \ldots$, the expression will increase by 1. This implies that

$$\{x\} = \frac{1}{k}, \frac{2}{k}, \ldots$$

are important points for us to consider.

Going back to the problem, we see that we have $k = 2, 4, 6, 8$ in our expression. This means that

$$\{x\} = \frac{1}{2}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{1}{6}, \ldots$$

are points to consider. However, we note that there may be overlap when the fraction can be simplified. If a fraction can be simplified, this means that its numerator and denominator are not relatively prime, which brings us to Euler!

We see that $\phi(2)+\phi(4)+\phi(6)+\phi(8) = 9$ is the number of fractions that cannot be simplified. However, we need to take into account $\frac{2}{6} = \frac{1}{3}$ and $\frac{4}{6} = \frac{2}{3}$ since while they can be simplified, they do not overlap with any of the other floor functions. Also, we need to include 0 for another case. This brings us to $9 + 2 + 1 = 12$ nonoverlapping changes in the expression $\lfloor 2\{x\} \rfloor + \lfloor 4\{x\} \rfloor + \lfloor 6\{x\} \rfloor + \lfloor 8\{x\} \rfloor$ for $0 \leq \{x\} < 1$.

Finally, we note that the question asks for integers between 1 and 1000, inclusive. Thus, we can have $20\lfloor x \rfloor = 0, 20, 40, \ldots, 980$ for a total of 50 cases for $\lfloor x \rfloor$. Note that although we can have $\lfloor x \rfloor = 50, \{x\} = 0$, we cannot have $\lfloor x \rfloor = 0, \{x\} = 0$, which is included in $20\lfloor x \rfloor = 0, 20, 40, \ldots, 980$. This adds and subtracts a case, canceling itself out.

Now, by doing some counting, there are 50 possibilities for $\lfloor x \rfloor$ and 12 for $\{x\}$, leading to $50 \cdot 12 = 600$ possible integers. ■

Exercise. If you know that $\phi(n) = k$, where n is some positive integer, then what is $\phi(n^2)$ in terms of n and k?

Exercise. Prove that the sum of all positive integers relatively prime to and less than an integer $n > 1$ is $\frac{n}{2}\phi(n)$. **Hint:** Consider pairing up integers k and $n - k$.

§16.3 Multiplicativity

Euler's Totient Function has a lot of interesting applications, especially in modular arithmetic, which you will learn about in a few days. Let's look at a separate property of the totient function:

Proposition 16.30. *If x and y are relatively prime integers, $\phi(x)\phi(y) = \phi(xy)$.*

Exercise. Prove this! Use the fact that if x and y are relatively prime, the sets of their prime divisors are disjoint.

Exercise. Try to come up with a formula for $\phi(xy)$ that covers instances when x and y are not relatively prime as well. Prove it if you want to.

We can consider $\phi(n)$ to be a **multiplicative** function over relatively prime integers. A multiplicative function f satisfies the relation $f(ab) = f(a)f(b)$ (where a and b are part of some

defined domain). An easy example would be $f(x) = x$. Surprisingly, we now know of two other multiplicative functions!

Proposition 16.31. *$\tau(n)$ and $\sigma(n)$ are multiplicative over relatively prime integers.*

Exercise. Prove this! The proof is extremely similar to proving that $\phi(n)$ is multiplicative over relatively prime integers.

This can be helpful for calculating different values.

Example 16.32. Let $x = 2^a$ and $y = 3^b$ for positive integers a, b. Verify that the totient function is multiplicative in this case; i.e. Proposition 16.30 holds.

Solution. First, we note that x and y are already in prime factorized form. Thus, applying the formula for the totient function gives us

$$\begin{aligned}\phi(x) &= 2^a \cdot \left(1 - \frac{1}{2}\right) \\ &= 2^{a-1}.\end{aligned}$$

Similarly,

$$\begin{aligned}\phi(y) &= 3^b \cdot \left(1 - \frac{1}{3}\right) \\ &= 2 \cdot 3^{b-1}.\end{aligned}$$

Thus, $\phi(x) \cdot \phi(y) = 2^a \cdot 3^{b-1}$. Now, since x and y are clearly relatively prime, we can calculate $\phi(xy)$ and see if it is equal to $\phi(x) \cdot \phi(y)$. Since $xy = 2^a \cdot 3^b$,

$$\begin{aligned}\phi(xy) &= 2^a \cdot 3^b \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \\ &= 2^a \cdot 3^b \cdot (\frac{1}{2})(\frac{2}{3}) \\ &= 2^a \cdot 3^{b-1}.\end{aligned}$$

Thus, Proposition 16.30 has been verified for this particular case of x, y. ■

Example 16.33. Given that $\phi(p) = 8$ and $\phi(q) = 18$, where p, q are relatively prime, find $\phi(pq)$.

Solution. By Proposition 16.30, we know that the totient function is multiplicative. Thus, $\phi(pq) = \phi(p) \cdot \phi(q) = 8 \cdot 18 = 144$. ■

Example 16.34. Compute $\phi(9!)$.

Solution. As usual, we first prime factorize 9!, giving

$$\begin{aligned}9! &= 9 \cdot 8 \cdots 2 \cdot 1 \\ &= 2^7 \cdot 3^4 \cdot 5 \cdot 7.\end{aligned}$$

Seeing these products, we use Proposition 16.30 to get

$$\begin{aligned}\phi(9!) &= \phi(2^7 \cdot 3^4 \cdot 5 \cdot 7) \\ &= \phi(2^7) \cdot \phi(3^4) \cdot \phi(5) \cdot \phi(7).\end{aligned}$$

Finally, we use the fact that $\phi(p^k) = p^{k-1}(p-1)$ to get

$$\begin{aligned}\phi(9!) &= \phi(2^7) \cdot \phi(3^4) \cdot \phi(5) \cdot \phi(7) \\ &= (2^6 \cdot 1) \cdot (3^3 \cdot 2) \cdot 4 \cdot 6 \\ &= 82944.\end{aligned}$$

■

§16.4 Homework Problems

Problem 16.1 (2007 PuMAC)**.** [4] If you multiply all positive integer factors of 24, you get 24^x. Find x.

Problem 16.2. [5] Given that $n = 36019$ and $\phi(n) = 35640$, find the sum of the 2 distinct prime factors of n.

Problem 16.3 (2013 AMC 10B)**.** [6] A positive integer n is nice if there is a positive integer m with exactly four positive divisors (including 1 and m) such that the sum of the four divisors is equal to n. How many numbers in the set $\{2010, 2011, 2012, \ldots, 2019\}$ are nice?

Problem 16.4 (2011 PUMaC)**.** [6] The only prime factors of an integer n are 2 and 3. If the sum of the divisors of n is 1815, find n.

Problem 16.5 (Brilliant)**.** [6] Let $\phi(n)$ be the Euler phi function. If $1 \leq n \leq 1000$, what is the smallest integer value of n that minimizes $\frac{\phi(n)}{n}$?

Problem 16.6 (2019 SMT)**.** [6] How many rational numbers can be written in the form $\frac{a}{b}$ such that a and b are relatively prime positive integers and the product of a and b is (25!)?

Problem 16.7. [6] Find the product of all primes p for which $17p + 9$ is a perfect square.

Problem 16.8 (2014 AIME I)**.** [6] Find the number of rational numbers r, $0 < r < 1$, such that when r is written as a fraction in lowest terms, the numerator and the denominator have a sum of 1000.

Problem 16.9 (2012 PuMAC)**.** [8] How many factors of $\left(20^{12}\right)^2$ less than 20^{12} are not factors of 20^{12}?

Problem 16.10 (2016 AMC 10B)**.** [8] Let $f(x) = \sum_{k=2}^{10}(\lfloor kx \rfloor - k\lfloor x \rfloor)$, where $\lfloor r \rfloor$ denotes the greatest integer less than or equal to r. How many distinct values does $f(x)$ assume for $x \geq 0$?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

17 Euclid's Algorithm, GCD and LCM

§17.1 GCD and LCM

Definition 17.1. The **greatest common divisor (GCD)** of two integers m, n is the largest integer d such that d divides both m and n.

Definition 17.2. The **least common multiple (LCM)** of two integers m, n is the smallest integer q such that both m and n divide q.

Definition 17.3. Two integers a, b are called **relatively prime** or coprime iff $\gcd(a, b) = 1$.

There are several ways of finding the GCD of two integers. Namely, Euclid's algorithm, discussed next section, does so.

However, the simplest way is to use prime factorizations. Let the prime factorizations of m and n be defined as

$$m = \prod_{i=1}^{\infty} p_i^{a_i} \qquad \text{and} \qquad n = \prod_{i=1}^{\infty} p_i^{b_i},$$

Where p_i is the ith prime and $a_i, b_i \geq 0$ for all i.

> *Remark.* Defining a_i, b_i as nonnegative rather than positive allows us to define m and n as such. They are not infinitely large; every exponent will be zero except for the primes actually contained in the factorization. We do this because it's much easier to then compare exponents of corresponding primes of m and n.

It is now much easier to find $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ with this notation.

For $d = \gcd(m.n)$, for every i,, the exponent of p_i in d must not exceed a_i or b_i. If not, then by the fundamental theorem of arithmetic, there cannot equal integer k such that $dk = m, n$.

Moreover, since d is large as possible, then for all i, the exponent of p_i must be exactly $\min a_i, b_i$. With this, we find that

$$d = \prod_{i=1}^{\infty} p_i^{\min\{a_i, b_i\}}.$$

To find $q = \operatorname{lcm}(m, n)$, the thinking is very similar. Instead, for all i, the exponent of p_i in q must be at least a_i, b_i, for $m, n|q$. Moreover, since q is minimal, then

$$q = \prod_{i=1}^{\infty} p_i^{\max\{a_i, b_i\}}.$$

This gives us an important property of GCD and LCM of two integers.

> **Proposition 17.4.** *For any positive integers m, n we have*
>
> $$\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn.$$

Proof. This should be clear given the above notations for d and q. If we simply use the previous notation, as described by the remark, it'll be much easier to compare exponents and then use the fundamental theorem of arithmetic.

> *Remark.* To prove two integers are equal, it greatly simplifies the problem if you consider their prime factorizations and show that the exponent of each prime in their respective prime factorizations are equal. This is true because of the fundamental theorem of arithmetic.

$$\gcd(m,n)\cdot \operatorname{lcm}(m,n) = \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}} \times \prod_{i=1}^{\infty} p_i^{\max\{a_i,b_i\}} = \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}+\max\{a_i,b_i\}}$$

Now, it suffices to show that

$$\prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}+\max\{a_i,b_i\}} = \prod_{i=1}^{\infty} p_i^{a_i+b_i}$$

As mentioned earlier, it's even simpler to just show each exponent for p_i is the same. In other words, all we have to do is show that

$$\min\{a_i,b_i\}+\max\{a_i,b_i\} = a_i + b_i.$$

This should be straightforward. It must be true that either $a_i \le b_i$ or $b_i \le a_i$. However, since the equation is symmetric in a_i and b_i (i.e swapping a_i and b_i does not change the equation), then we can say, "Without loss of generality", and assume that $a_i \le b_i$.

Then, it is clear that $\min\{a_i,b_i\} = a_i$ and $\max\{a_i,b_i\} = b_i$, implying that

$$\min\{a_i,b_i\}+\max\{a_i,b_i\} = a_i + b_i,$$

as desired. ■

> *Remark.* In summary, we did the following steps in our proof:
>
> - We used the fact that
>
> $$m = \prod_{i=1}^{\infty} p_i^{a_i} \qquad \text{and} \qquad n = \prod_{i=1}^{\infty} p_i^{b_i}.$$
>
> - We exploited the fundamental theorem of arithmetic to show that the exponent of every prime in the prime factorization of both sides equation were the same
> - We concluded that because either $a_i \le b_i$ or $b_i \le a_i$ that then $\min\{a_i,b_i\}+\max\{a_i,b_i\} = a_i + b_i$.
> - By the fundamental theorem of arithmetic, we then conclude that the two numbers are indeed equal.

Exercise. Prove that $\gcd(a,b,c) = \gcd(\gcd(a,b),c)$.

> **Example 17.5.** Let a and b be positive integers such that
>
> $$\gcd(a^2,b^2)\cdot \operatorname{lcm}(a,b) - 5ab = 6\operatorname{lcm}(a,b)$$

Assume that $\gcd(a,b)$ is positive. What is the $\gcd(a^4,b^4)$?

Solution. On the left side of the equation, we have a product of a GCD and LCM, along with the product ab. This motivates us to consider $ab = \gcd(a,b)\cdot\operatorname{lcm}(a,b)$, giving the equation is

$$\gcd(a^2,b^2)\cdot\operatorname{lcm}(a,b) - 5\gcd(a,b)\cdot\operatorname{lcm}(a,b) = 6\operatorname{lcm}(a,b)$$

We may now simply divide a factor of $\operatorname{lcm}(a,b)$ to get

$$\gcd(a^2,b^2) - 5\gcd(a,b) - 6 = 0.$$

This almost seems to be a quadratic in terms of $\gcd(a,b)$, but unfortunately we have $\gcd(a^2,b^2)$ instead of $\gcd(a,b)^2$. Thus instead, we should try to see if there exists some relationship between $\gcd(a^2,b^2)$ and $\gcd(a,b)^2$.

How would we do such a thing? Why, using the definition of the GCD, of course! First, we compute $\gcd(a,b)^2$ as

$$\prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}} \times \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}} = \prod_{i=1}^{\infty} p_i^{2\min\{a_i,b_i\}}.$$

Similarly, note that the factorization for a^2 and b^2 are, respectively,

$$\prod_{i=1}^{\infty} p_i^{2a_i} \qquad \text{and} \qquad \prod_{i=1}^{\infty} p_i^{2b_i}.$$

Hence, this implies that

$$\gcd(a^2,b^2) = \prod_{i=1}^{\infty} p_i^{\min\{2a_i,2b_i\}}.$$

Like we did previously, let's compare the individual exponents of each prime. Like last time, note that by symmetry, we can without loss of generality let $a_i \le b_i$. Then,

$$2\min\{a_i,b_i\} = 2a_i.$$

Similarly, since $a_i \le b_i$, then $2a_i \le 2b_i$, so we find

$$\min\{2a_i,2b_i\} = 2a_i,$$

Meaning that in fact, $2\min\{a_i,b_i\} = \min\{2a_i,2b_i\}$. Then, by the fundamental theorem of arithmetic, we can conclude that

$$\gcd(a^2,b^2) = \prod_{i=1}^{\infty} p_i^{\min\{2a_i,2b_i\}} = \gcd(a^2,b^2) = \prod_{i=1}^{\infty} p_i^{2\min\{a_i,b_i\}} = \gcd(a,b)^2!$$

Now, substituting into our original equation gives the quadratic

$$\gcd(a,b)^2 - 5\gcd(a,b) - 6 = 0.$$

This conveniently factors as

$$(\gcd(a,b) - 6)(\gcd(a,b) + 1) = 0.$$

Clearly, $\gcd(a,b) > 0$, so this gives that $\gcd(a,b) = 6$. Now, with the exact same reasoning as before, $\gcd(a^4,b^4) = \gcd(a,b)^4$, meaning that our desired answer is $\gcd(a,b)^4 = 6^4 = \boxed{1296}$. ■

Example 17.6 (2018 AMC). How many ordered pairs (a, b) of positive integers satisfy the equation

$$a \cdot b + 63 = 20 \cdot \text{lcm}(a, b) + 12 \cdot \gcd(a, b),$$

where $\gcd(a, b)$ denotes the greatest common divisor of a and b, and $\text{lcm}(a, b)$ denotes their least common multiple?

Solution. This should look familiar now. We have an equation in terms of $\text{lcm}(a, b)$ and $\gcd(a, b)$ as well as the product ab. Thus, in order to get everything in terms of $\text{lcm}(a, b)$ and $\gcd(a, b)$, we can substitute $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

$$\gcd(a, b) \cdot \text{lcm}(a, b) + 63 = 20 \cdot \text{lcm}(a, b) + 12 \gcd(a, b).$$

We may rearranged the equation to move all of the $\text{lcm}(a, b)$ and $\gcd(a, b)$ on one side and constants on the other as

$$\gcd(a, b) \cdot \text{lcm}(a, b) - 20 \cdot \text{lcm}(a, b) - 12 \gcd(a, b) = -63.$$

We now use the colloquial "Simon's Favorite Factoring Trick (SFFT)". Where we ultimately want to incorporate the product $(\gcd(a, b) - 20)(\text{lcm}(a, b) - 12)$ into the equation.

Remark. In general, Simon's Favorite Factoring Trick states that

$$xy + xk + yj + jk = (x + j)(y + k)$$

Hence, if you ever see an expression of the form $xy+xk+yj$, it may be helpful to manipulate the constant term to achieve such a factoring.

Thus, since

$$(\gcd(a, b) - 20)(\text{lcm}(a, b) - 12) = \gcd(a, b) \cdot \text{lcm}(a, b) - 20 \cdot \text{lcm}(a, b) - 12 \gcd(a, b) + 240,$$

We should add 240 to both sides of the previous equation to yield

$$(\gcd(a, b) - 20)(\text{lcm}(a, b) - 12) = 240 - 63 = 177.$$

Now, we have a product of integers equalling 177, so we must consider all possible pairs of integers multiplying to 177. These are:

$$\begin{aligned} 177 &= 177 \times 1 \\ 177 &= 59 \times 3 \\ 177 &= (-59) \times (-3) \\ 177 &= (-177) \times (-1) \end{aligned}$$

However, right away, we can eliminate cases 3 and 4, for they would result in either $\gcd(a, b)$ or $\text{lcm}(a, b)$ to be less than 0.

Moreover, note that $\gcd(a, b) \leq \text{lcm}(a, b)$, meaning that $\gcd(a, b) - 20 < \text{lcm}(a, b) - 12$.

Case 1: $\text{lcm}(a, b) - 12 = 177$ and $\gcd(a, b) - 20 = 1$.

Clearly, then $\text{lcm}(a,b) = 189$ and $\gcd(a,b) = 21$. As a result, by definition, since $\gcd(a,b) = 21$, then $a = 21a'$ and $b = 21b'$ where $\gcd(a',b') = 1$. (Note: had it been true that $\gcd(a',b') = k > 1$, then $\gcd(a,b) = 21k$.)

Then, $\text{lcm}(a,b) = 21a'b' = 189$, meaning that we must find a', b' such that $a'b' = 9$ and $a'b'$ are relatively prime. This has two ordered pairs of $(1,9)$ and $(9,1)$, giving $\boxed{2}$ ordered pairs.

Case 2: $\text{lcm}(a,b) - 12 = 59$ and $\gcd(a,b) - 20 = 3$.

Clearly, then $\text{lcm}(a,b) = 71$ and $\gcd(a,b) = 23$. As a result, by definition, since $\gcd(a,b) = 23$, then $a = 23a'$ and $b = 23b'$ where $\gcd(a',b') = 1$.

Then, $\text{lcm}(a,b) = 23a'b' = 71$. However, $23 \nmid 71$, resulting in a contradiction. Thus, there are $\boxed{0}$ ordered pairs for this case.

In conclusion, from both cases, there exists only $2 + 0 = \boxed{2}$ ordered pairs satisfying the given conditions, namely $(189, 21)$ and $(21, 189)$. ■

Exercise 17.7. How many ordered pairs of integers (a,b) satisfy

$$\gcd(a,b) = 20 \qquad \text{and} \qquad \text{lcm}(a,b) = 180?$$

Exercise 17.8 (CMC Year 3). How many ordered triples (a,b,c) of not necessarily distinct positive integer divisors of $216,000$ satisfy

$$\text{lcm}(a, \gcd(b,c)) = \text{lcm}(b, \gcd(a,c)) = \text{lcm}(c, \gcd(a,b))?$$

§17.2 Euclidean Algorithm

Before we get into the Euclidean Algorithm, we first need to start with the division algorithm.

Definition 17.9. The **division algorithm** takes two positive integers and returns the quotient and remainder when one divides the other. The algorithm starts with the two numbers and takes the divisor (this is the number that is "doing the dividing") and finds the largest multiple of the divisor which is less than or equal to the dividend (the number "being divided").

Once you find this multiple, the number that you multiplied the divisor by is the **quotient**, the difference between the multiple that was found and the dividend is the **remainder**.

Mathematically, if we have an integer a and are dividing by b, then the division algorithm finds us an integer q (the quotient) and an integer r (the remainder) such that $0 \leq r < b$ and $a = bq + r$.

Definition 17.10. The **Euclidean Algorithm** finds the GCD of two numbers by using the division algorithm until you either get that one number is the multiple of another or that the GCD of the numbers is 1. First you start with the two numbers you want, then use the division algorithm where the smaller number is set as the divisor and the larger number is the dividend, then get the remainder r as defined above.

If the remainder is 0 then one number is a multiple of the other and the GCD of the two numbers is the smaller of the two numbers; if the remainder is 1 the GCD of the two numbers is 1. otherwise replace the larger of the two numbers with the remainder you found.

Mathematically, letting $a = bq + r$ as described in the division algorithm, the Euclidean algorithm uses the fact that $\gcd(a, b) = \gcd(r, b)$ repeatedly.

It may not seem evident how this ends up working, but once we do some examples it should be easier to understand. Before we get into the examples, though, we encourage you to prove the following statement:

Exercise. Prove that if a and b are integers such that $a > b$, then $\gcd(a, b) = \gcd(a - b, a)$.

The reason the Euclidean algorithm works actually boils down to this simple fact; letting $a = bq + r$ as described in the division algorithm, we have that

$$\gcd(a, b) = \gcd(bq + r, b) = \gcd(b(q - 1) + r, b) = \cdots = \gcd(r, b)$$

which is the fundamental assumption of the Euclidean algorithm.

For finding the GCD of two given integers, using division at each step is the fastest method, but if we are trying to find the GCD of algebraic expressions its often simpler to just reduce using the fact that $\gcd(a, b) = \gcd(a - b, a)$.

Now we'll get into the examples.

Example 17.11. Find the GCD of 1003 and 68.

Solution. Now we perform the Euclidean Algorithm:

$$\begin{aligned} 1003 &= 68 \cdot 14 + 51 \\ 68 &= 51 \cdot 1 + 17 \\ 51 &= 17 \cdot 3 + 0 \end{aligned}$$

Note that in each subsequent step, we take the divisor from the previous step and use the remainder from the previous step as our new divisor. We stop once we reach 0.

The first equation in our Euclidean algorithm signifies that $\gcd(1003, 68) = \gcd(51, 68)$. The second signifies that $\gcd(51, 68) = \gcd(51, 17)$, and the last equation signifies that $\gcd(51, 17) = \gcd(17, 0)$, which we know is 17. Thus, $\gcd(1003, 68) = \gcd(51, 68) = \gcd(51, 17) = \gcd(17, 0) = 17$. ■

Example 17.12. Find the GCD of 2002 and 78.

Solution.

$$\begin{aligned} 2002 &= 25 \cdot 78 + 52 \\ 78 &= 1 \cdot 52 + 26 \\ 52 &= 2 \cdot 26 + 0 \end{aligned}$$

This is done in the same way as the previous example. The first equation tells us that $\gcd(2002, 78) = \gcd(52, 78)$. The second equation then tells us that $\gcd(52, 78) = \gcd(52, 26)$. The last equations tells us that $\gcd(52, 26) = 26$ since 52 is a multiple of 26. From these three equations we see that $\gcd(2002, 78) = \gcd(52, 78) = \gcd(52, 26) = 26$. ■

Example 17.13 (1959 AIME). Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

Solution. We will prove that $\gcd(21n+4, 14n+3) = 1$. Using the Euclidean algorithm gives

$$\gcd(21n+4, 14n+3) = \gcd(7n+1, 14n+3) = \gcd(7n+1, 1) = 1.$$

Thus, our claim was proven and we are done. ■

Example 17.14 (1985 AIME). The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Solution. From the given information, we have that

$$d_n = \gcd(a_n, a_{n+1}) = \gcd(100 + n^2, 100 + n^2 + 2n + 1).$$

We notice that we can use the Euclidean algorithm here to find the GCD; we just need to figure out how to cancel out all the terms with n. Applying the Euclidean algorithm once gives

$$\gcd(100 + n^2, 100 + n^2 + 2n + 1) = \gcd(100 + n^2, 2n + 1).$$

Now we want to cancel out the n^2 term, and we must do so by subtracting a multiple of $2n+1$. We can subtract $\frac{n}{2}(2n+1)$, to cancel it, but how do we know if $\frac{n}{2}$ is an integer? It depends on whether n is even or odd. We could just do casework based on the parity of n, but there's a faster solution; we know that $2n+1$ is odd, so

$$\gcd(100 + n^2, 2n + 1) = \gcd(200 + 2n^2, 2n + 1)$$

since changing the even factors of the left integer won't change the gcd. Then we can subtract $n(2n+1)$ which gives

$$\gcd(200 + 2n^2 - n(2n+1), 2n + 1) = \gcd(200 - n, 2n + 1)$$

Finally, we can add $2(200-n)$ to the right integer and get $d_n = \gcd(200-n, 401)$. We've finally got a constant value. Then the maximum possible value of d_n is 401, which is achievable by taking $n = 601$, so our answer is 401. ■

Exercise 17.15. Find $\gcd(999, 148)$.

Exercise 17.16. Find $\gcd(20, 45, 36)$ using the Euclidean Algorithm.

§17.3 Homework Problems

Problem 17.1. [3] Let $I + 3 = WM$ for positive integers I, W, M such that $W + M = 6$. Find the sum of all distinct values of $\gcd(I^3, W^M)$.

Problem 17.2. [4] Find $\gcd(999999, 6512)$ using the Euclidean Algorithm.

Problem 17.3 (2013 AMC 8)**.** [4] What is the ratio of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594?

Problem 17.4 (2016 AMC 8)**.** [5] The least common multiple of a and b is 12, and the least common multiple of b and c is 15. What is the least possible value of the least common multiple of a and c?

Problem 17.5 (2020 AMC 10 A)**.** [6] Let n be the least positive integer greater than 1000 for which

$$\gcd(63, n + 120) = 21 \quad \text{and} \quad \gcd(n + 63, 120) = 60.$$

What is the sum of the digits of n?

Problem 17.6 (2019 PUMAC)**.** [6] The least common multiple of two integers a and b is $2^5 \times 3^5$. How many such ordered pairs (a, b) are there?

Problem 17.7 (2016 AMC 10/12A)**.** [7] How many ordered triples (x, y, z) of positive integers satisfy $\text{lcm}(x, y) = 72$, $\text{lcm}(x, z) = 600$, and $\text{lcm}(y, z) = 900$?

Problem 17.8 (2017 CMIMC)**.** [7] Determine the sum of all possible values of $m + n$, where m and n are positive integers satisfying

$$\text{lcm}(m, n) - \gcd(m, n) = 103.$$

Problem 17.9 (2018 PUMaC)**.** [8] Let n be a positive integer. Let $f(n)$ be the probability that, if divisors a, b, c of n are selected uniformly at random with replacement, then $\gcd(a, \text{lcm}(b, c)) = \text{lcm}(a, \gcd(b, c))$. Let $s(n)$ be the sum of the distinct prime divisors of n. If $f(n) < \frac{1}{2018}$, compute the smallest possible value of $s(n)$.

Problem 17.10 (2020 AMC 12A)**.** [6] How many positive integers n are there such that n is a multiple of 5, and the least common multiple of 5! and n equals 5 times the greatest common divisor of 10! and n?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

18 Modular Arithmetic, Linear Congruences, and Divisibility Rules

§18.1 Modular Arithmetic

The motivation of modular arithmetic is to simplify problems involving remainders. Consider the following problem:

Example 18.1. What is the remainder when 6^{2020} is divided by 5?

Solution. Assume that you have no idea what modular arithmetic is. Recall the binomial theorem, which details the expansion of $(a+b)^n$. Let's rewrite 6 as $5+1$, so the problem changes to: the remainder when $(5+1)^{2020}$ is divided by 5. Then, the binomial theorem tells us that the expanded version of this is

$$5^{2020} + \binom{2020}{2019}5^{2019}1^1 + \binom{2020}{2018}5^{2018}1^2 + \cdots + \binom{2020}{1}5^1 1^{2019} + 1^{2020}.$$

Every term in this expansion except for the last has a factor of 5 in it, so the remainder when this is divided by 5 will just be equal to 1. ■

It doesn't seem like a coincidence that the remainder of 6 divided by 5 is equal to 1, and the remainder of 6^{2020} when divided by 5 is equal to 1^{2020}. Let's try to formalize this notion by introducing the concept of **modular arithmetic**.

We say that two integers a, b are **congruent modulo n** (modulo is sometimes shortened to mod) if $a-b$ is divisible by n, and we denote this as $a \equiv b \pmod{n}$. (Read: a is congruent to b mod n.) (Recall that we say $a \mid b$ if there is some integer c such that $ac = b$.) We refer to n as the **modulus**. We can heuristically think of a and b as leaving the same remainder when divided by n.

Going back to the first example, we can write

$$6^{2020} \equiv 1 \pmod{5},$$

pronounced as "6^{2020} is congruent to 1 modulo 5." Note that the $\equiv$ sign means "congruent," so we refer to these statements as **congruences**.

Now we'll introduce some properties of modular arithmetic. You'll start to see that congruences share many properties with equations, such as addition, subtraction, and multiplication to both sides preserving it. Try to think about these properties in terms of remainders and the formal definition.

- $a \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
- a is a multiple of n if and only if $a \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$

- If $a \equiv b \pmod{n}$, then $am \equiv bm \pmod{n}$
- If $ma \equiv mb \pmod{n}$, then $a \equiv b \pmod{n/\gcd(m,n)}$
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$

Exercise. Prove the above properties using our definition of congruence modulo n.

Example 18.2. Prove that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Solution. Note that $n \mid a-b$ by the definition of modular arithmetic, and $a-b \mid a^k-b^k$. Thus $n \mid a^k - b^k$, as desired. ■

Remark. This property applies to our earlier example. Instead of going through the entire binomial theorem, we can simply say that since $6-1$ is divisible by 5, then we have $6 \equiv 1 \pmod{5} \implies 6^{2020} \equiv 1^{2020} \equiv 1 \pmod{5}$.

In the context of this problem and plenty of other MATHCOUNTS remainder problems, it is helpful to define a **least residue.**

Definition 18.3. The least residue of $a \pmod{n}$ is the the value of l with $0 \le l \le n-1$ such that $a \equiv l \pmod{n}$. In common language, l is just the "remainder" when a is divided by n.

Example 18.4. Pi day this year (2020) was on Saturday, March 14. On what day of the week will Pi day be, in 2023?

Solution. We don't have to worry about leap years (since February of 2020 passed before Pi day), so we know that there will be $3 \cdot 365 = 1095$ days until Pi day 2023. Since the days of the week repeat every 7 days, the answer is essentially the least residue of 1095 mod 7, converted into the day of the week.

We could use long division, but we could also find this least residue by subtracting obvious multiples of 7 until we get a number small enough. For example, 700 is a multiple of 7, so we have $1095 \equiv 1095 - 700 \equiv 395 \pmod{7}$. Continuing, $395 \equiv 395 - 350 \equiv 45 \equiv 3 \pmod{7}$. Therefore, the day of the week will be 3 days after Saturday, or $\boxed{\text{Tuesday}}$. ■

Example 18.5 (MATHCOUNTS 2016). What is the remainder when $1^2+2^2+3^2+\cdots+2016^2$ is divided by 17?

Solution. We know that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

from algebra. Thus, the sum from the problem turns into

$$\frac{2016(2017)(4033)}{6} = 336 \cdot 2017 \cdot 4033.$$

Now, we compute the least residues of each of these three numbers.

$$336 \equiv 13 \pmod{17}, \quad 2017 \equiv 2017 - 1700 \equiv 317 \equiv 11 \pmod{17},$$

and

$$4033 \equiv 2(2017) - 1 \equiv 2(11) - 1 \equiv 21 \equiv 4 \pmod{17}.$$

Multiplying these numbers back together, we obtain

$$13 \cdot 11 \cdot 4 \equiv 143 \cdot 4 \equiv 7 \cdot 4 \equiv 11 \pmod{17},$$

and the remainder is $\boxed{11}$. ■

§18.1.1 Negative Residues in Modular Arithmetic

So far, we've only worked with positive residues in modular arithmetic. But what about negative residues? Recall the formal definition: two numbers a, b are congruent modulo n if $a - b = kn$, for some integer k. This definition can be thought as: "If the difference between two numbers is divisible by n, then they are congruent mod n."

If a or b are negative, then that's fine, as long as their difference is divisible by n. Negative numbers also follow all of the earlier properties. A common misconception is that $a \equiv -a \pmod{n}$. This is not necessarily true, since this does not necessarily follow the formal definition. Let's do an example.

Example 18.6. Find a if $a \equiv 30 \pmod{13}$ and a is the greatest negative integer that satisfies the congruence.

Solution. We have that the difference between 30 and a must be divisible by 13. In other words, $30 - a = 13k$. Since we know that a is negative, then on the LHS, we are essentially subtracting a negative number, or adding. Therefore, the greatest negative value for a is $\boxed{-9}$. ■

In general, we can easily see that if $a \neq 0$ is some least residue modulo n, then the least residue corresponding to $-a$ is simply $n - a$.

Example 18.7. Determine whether each of the following pairs of integers is congruent modulo 9:

1. $(-1, 899)$
2. $(-17, -171)$
3. $(-90, 900)$
4. $(-55, 755)$

Solution. For two numbers to be congruent mod 9, their difference must be divisible by 9. For the first pair, the difference is 900 or -900, depending on which way you subtract. Either way, this difference is divisible by 9, so we have $-1 \equiv 899 \pmod{9}$.

For the second pair, the difference is $154 = 14 \times 11$, which is not divisible by 9, so we can write $-17 \not\equiv -171 \pmod{9}$.

For the third pair, the difference is 990, so we have $-90 \equiv 900 \pmod{9}$.

For the fourth pair, the difference is 810, we have $-55 \equiv 755 \pmod{9}$. ■

Now, let's see how using residues numbers could be helpful:

Example 18.8. What is the units digit of $17^7 + 18^8$?

Solution. How do we find the units digit of something using modular arithmetic? Note that the units digit of any number m is equal to the remainder when m is divided by 10. In other words, it is the least residue of $m \pmod{10}$.

Now, we're ready to tackle this problem. Let's break it up. First, we find the units digit of 17^7.

We have $17^7 \equiv 7^7 \pmod{10}$. Notice that $7^2 \equiv -1 \pmod{10} \implies 7^7 \equiv (7^6)7 \equiv (-1)^3 \cdot 7 \equiv 3 \pmod{10}$.

Now, we focus on the 18^8. We have $18^8 \equiv 8^8 \equiv (-2)^8 \equiv (-2)^4(-2)^4 \equiv 16 \cdot 16 \equiv 6 \cdot 6 \equiv 6 \pmod{10}$. Therefore, $17^7 + 18^8 \equiv 3 + 6 \equiv 9 \pmod{10}$. ■

Notice how we used negative numbers to significantly reduce the numbers that we were working with, in order to simplify calculations and to arrive at an answer quicker.

§18.1.2 Modular inverses

You might notice that we've stayed away from division thus far. This is because division is quite weird in modular arithmetic.

Definition 18.9. A **multiplicative inverse of a modulo n** is denoted as a^{-1} (you might also sometimes see $\overline{a}$), and satisfies $a \cdot a^{-1} \equiv 1 \pmod{n}$.

This is an important concept because 1 is a very nice number to work with, especially when dealing with multiplication of big numbers or exponents, and it will also help us understand linear congruences better. More on that later.

It is also important because in situations where we might divide both sides when we're solving an equation, we might not be able to do that in a congruence without tweaking the modulus or making other changes. Thus, we introduce the inverse as a way to remedy this; **instead of dividing both sides, we multiply both sides by an inverse.**

However, modular inverses do not always exist. We'll go into when they do later in the section.

Finally, note that if b is the inverse of a modulo n, then any other value in the same residue class as b would also be an inverse of a. In terms of congruences, if

$$ab \equiv 1 \pmod{n} \text{ and } b \equiv c \pmod{n} \implies ac \equiv 1 \pmod{n} \implies b \equiv c \equiv a^{-1} \pmod{n}.$$

You have to be careful when stating $a^{-1} \equiv \frac{1}{a}$. Fractions and rational numbers are not well-defined with remainders and modular arithmetic, so it's always best to prove statements such as $\frac{1}{a} + \frac{1}{b} \equiv \frac{a+b}{ab} \pmod{n}$. Grading issues have occurred in olympiads because of this, so we present an example that properly uses addition of inverses.

Feel free to ignore this example if you do not know Fermat's Little Theorem. This example is absolutely not essential.

Example 18.10 (2005 IMO). Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$

Solution. We claim the answer is just 1. It is easy to show that it works.

Note that $a_2 = 12$, showing 2 and 3 do not work.

Now we just show that $2^{p-1} + 3^{p-1} + 6^{p-1} - 1 \equiv 0 \pmod{p}$. This heuristically should work since

$$2^{p-1} + 3^{p-1} + 6^{p-1} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p}.$$

Now we have to show that $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \equiv 1 \pmod{p}$ is valid.

We claim that in general, $a^{-1} + b^{-1} \equiv (a+b)(a^{-1}b^{-1}) \pmod{p}$. Note that by the distributive property, $(a+b)(a^{-1}b^{-1}) \equiv aa^{-1}b^{-1} + bb^{-1}a^{-1} \equiv b^{-1} + a^{-1} \pmod{p}$, so adding fractions is valid. ■

When working with congruences, it's important to keep in mind that we're always working in integers. Fractions are just a convenient shorthand that happen to work - you must keep in mind why and when they do.

Example 18.11. Find the inverse of 2, 12, and 5 modulo 55.

Solution. Let's start with finding 2^{-1}. We want to find a number x such that $2x \equiv 1 \pmod{55}$. You might observe that $x = 28$ works because $2 \cdot 28 = 56 \equiv 1 \pmod{55}$, so we know that any number congruent to 28 modulo 55 would be an inverse of 2.

There is a more rigorous approach for finding modular inverses using the Euclidean algorithm. Recall that modular arithmetic is fundamentally just another way to represent remainders. When working with modular arithmetic, don't forget that in the end, we're ultimately dealing with a division problem.

Now let's find 12^{-1}. We want to find a solution for x in the congruence $12x \equiv 1 \pmod{55}$. In other words, we want to find integer solutions for the equation $12x = 55q+1 \implies 12x-55q = 1$. Now, we'll illustrate how to use the Euclidean algorithm:

$$\begin{aligned} 55 &= 12 \cdot 4 + 7 & \gcd(55, 12) \\ 12 &= 7 \cdot 1 + 5 & = \gcd(7, 12) \\ 7 &= 5 \cdot 1 + 2 & = \gcd(7, 5) \\ 5 &= 2 \cdot 2 + 1 & = \gcd(2, 5). \end{aligned}$$

Note that we ended with 1; this is no coincidence, but we'll clear this up later. Because we have a 1, we can backtrack to express it as a linear combination of 12 and 55:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7 - 5 \cdot 1) \\ &= 5 \cdot 3 - 2 \cdot 7 \\ &= (12 - 7 \cdot 1) \cdot 3 - 2 \cdot 7 \\ &= 12 \cdot 3 - 5 \cdot 7 \\ &= 12 \cdot 3 - 5(55 - 12 \cdot 4) \\ &= 12 \cdot 23 - 55 \cdot 5. \end{aligned}$$

Thus, $x = 23$ and $q = 5$, and the inverse of 12 modulo 55 is any number congruent to 23 modulo 55. Notice how we used the equations that we found using the Euclidean Algorithm

and substitution to arrive at an answer. Besides finding the gcd of two very big numbers, this is one of the many applications of the Euclidean Algorithm.

Now, to find 5^{-1}. We can use the same technique, and write the equation $5x = 55q + 1 \implies 5x - 55q = 1 \implies 5(x - 11q) = 1 \implies x - 11q = \frac{1}{5}$. Hold on. There's no way we can find integers x and q such that $x - 11q$ is a fraction! What does this mean? This means that 5^{-1} simply does not exist. There is no number that we can multiply to 5 in order to obtain a number that is congruent to 1 mod 55. ■

This raises the question: When does a^{-1} modulo n exist?

Proposition 18.12. *a^{-1} exists modulo n. iff $\gcd(a, n) = 1$.*

Proof. First we'll prove the forwards direction (i.e. that the first statement implies the second). Suppose to the contrary that $g = \gcd(a, n) > 1$. We want to show that there are no solutions for x in the congruence

$$ax \equiv 1 \pmod{n}.$$

We can use the same strategy as before and write out the equation: $ax = 1+qn \implies ax-qn = 1$. Don't forget that a, x, q, and n are all integers! We factor out a g on the LHS, so our new equation becomes

$$g\left(\frac{a}{g}x - \frac{n}{g}q\right) = 1 \implies \frac{a}{g}x - \frac{n}{g}q = \frac{1}{g}.$$

However, by definition, g is a factor of both a and n, so we know that $\frac{a}{g}$ and $\frac{n}{g}$ are both integers. Therefore, the LHS must be an integer. The RHS will not be an integer because $g > 1$, and thus we have reached a contradiction.

For the reverse direction, note that the Euclidean algorithm with a and n must terminate in 1 (the gcd of the two numbers), so backtracking will give us a linear combination $ax + ny = 1$, where x will be our desired a^{-1}. ■

Exercise. Make the argument for the reverse direction more rigorous using the Euclidean algorithm and strong induction.

Remark. Note that this means that any nonzero residue mod a prime p will have an inverse; this is handy to remember since we'll often be working with a prime modulus in problems.

Proposition 18.13. *If the multiplicative inverse of a exists modulo n, then exactly one value between 0 and $n - 1$ is an inverse of a. In other words, if a has an inverse, then it is unique modulo n.*

Proof. Suppose to the contrary that the inverse of a exists and there exist two values i, j, such that $0 \le i < j \le n - 1$, and $aj \equiv ai \equiv 1 \pmod{n}$. Combining, we have

$$aj \equiv ai \pmod{n} \implies a(j - i) \equiv 0 \pmod{n}.$$

Since a has an inverse, then $\gcd(a, n) = 1$. However, we must have $a(j - i)$ as a multiple of n, so we conclude that $j - i$ is a multiple of n. By construction, $j - i \le n - 1$, so we have arrived at a contradiction. ■

Example 18.14. Given that p is a prime, for which integer values of a between 0 and $p-1$, inclusive, satisfy the property that a is its own inverse?

Solution. Recalling the definition, we want to find all values of a for which $a \cdot a \equiv 1 \pmod{p} \implies a^2 \equiv 1 \pmod{p} \implies a^2 - 1 \equiv 0 \pmod{p} \implies (a+1)(a-1) \equiv 0 \pmod{p}$. From this, we see that either $a+1$ or $a-1$ must be a multiple of p. Since we are restricted by $0 \leq a \leq p-1$, our only possible values for a would be $a = p-1$ and $a = 1$. ■

Remark. It should be noted that the integers modulo n are divided into n distinct **residue classes**. Each residue class is a set of integers that are all congruent to each other modulo n.

§18.1.3 Exercises for this section

Exercise 18.15. What time does a clock read 100 hours after it reads 2 o' clock? (The clock is an analog, 12-hour clock)

Exercise 18.16. Find the remainder when 2^{12} is divided by 13. **Hint:** Build up! $2^{12} \equiv 2^8 \cdot 2^4$, and $2^8 \equiv (2^4)^2$.

Exercise 18.17. Find the remainder when 10! is divided by 11. **Hint:** Use some negative numbers to simplify calculations.

Exercise 18.18. Determine which integers a where $1 \leq a \leq 24$ have an inverse modulo 24.

Exercise 18.19. For which positive integers n is it true that

$$\sum_{i=1}^{n-1} i^2 \equiv 0 \pmod{n}?$$

What about if n satisfies

$$\sum_{i=1}^{n-1} i^3 \equiv 0 \pmod{n}$$

instead?

Exercise 18.20. Prove that if p is a prime number, and x and y are positive integers such that $x \equiv y \pmod{p}$, then $x^p \equiv y^p \pmod{p^2}$. **Hint:** Move everything to one side. Now what can we do?

§18.2 Linear Congruences

A congruence in the form

$$ax \equiv b \pmod{n}$$

is called a **linear congruence**, for positive integers a, b, n, because the degree of x is 1. In this congruence, we want to solve for x, which is also an integer.

Similar to inverses, if x_0 is a solution to the congruence $ax \equiv b \pmod{n}$ for x, then any other number in the same residue class as x_0 is also a solution.

Now, when does this not have a solution for x? Let's consider the congruence

$$2x \equiv 1 \pmod 6.$$

Doing a quick analysis, we see that $2x$ is always an even number, and that it must be 1 more than a multiple of 6. Well, any number that's congruent to 1 modulo 6 must be odd, so there aren't any solutions to this linear congruence. This raises the question: When does a linear congruence have a solution for x? Let's do some examples to get more comfy with the idea of linear congruences.

Example 18.21. Solve for x if $2x \equiv 3 \pmod 5$.

Solution. We've solved linear congruences before when we dealt with inverses, you just didn't know that they were called linear congruences until now. Recall how we introduced inverses as an alternative to division in modular arithmetic. Normally, to solve the equation $2x = 3$, you would just divide by sides by 2, to get $x = \frac{3}{2}$. However, modular arithmetic and fractions don't go together! Let's use inverses here. Then, we have

$$2x \equiv 3 \pmod 5 \implies 2x \cdot 2^{-1} \equiv 3 \cdot 2^{-1} \pmod 5 \implies x \equiv 4 \pmod 5,$$

because $2 \cdot 2^{-1} \equiv 1 \pmod 5$, and $2^{-1} \equiv 3 \pmod 5$. Thus any number congruent to 4 (mod 5) is a solution to the congruence. ■

Hmmm, so this congruence had a solution, but our earlier one ($2x \equiv 1 \pmod 6$) did not. You might suspect that it's because we needed to multiply both sides by 2^{-1} in order to isolate x, and that $\gcd(2, 6) \neq 1$, so the inverse of 2 doesn't exist. Let's see how we might need to modify this argument...

Example 18.22. Solve for x in the congruence $9x \equiv 12 \pmod{15}$.

Solution. Here, $\gcd(9, 15) \neq 1$, so by our previous argument, this congruence should not have a solution. However, recall that we can divide both sides by 3, so we get

$$9x \equiv 12 \pmod{15} \implies \frac{9}{3}x \equiv \frac{12}{3} \pmod{15/\gcd(3, 15)} \implies 3x \equiv 4 \pmod 5.$$

Now, this congruence has a solution: $x \equiv 3 \pmod 5$. Let's list some actual concrete numbers that x could be: $x = 3, 8, 13, 18, 23, \ldots$ Looking back at the original problem, we see that the original modulus was 15, and $3 \not\equiv 8 \not\equiv 13 \pmod{15}$, which means that x has three different solutions modulo 15! ■

This example brings us to the following proposition:

Proposition 18.23. *Consider the linear congruence*

$$ax \equiv b \pmod n$$

and let $\gcd(a, n) = g$. *If* $g \nmid b$, *then no solutions exist. Otherwise, the congruence has* g *distinct solutions modulo* n.

§18.2.1 Exercises for this section

Exercise 18.24. Verify that Proposition 5.21 holds for the three examples in this section.

Exercise 18.25. Solve for x in the congruence $5x + 7 \equiv 9 \pmod{11}$.

§18.3 Divisibility Rules

The last part of this handout deals with a direct application of modular arithmetic: divisibility rules. Let's recap with some basic information. We use a base 10 number system, which means that the number $478 = 4 \cdot 100 + 7 \cdot 10 + 8 \cdot 1 = 4 \cdot 10^2 + 7 \cdot 10^1 + 8 \cdot 10^0$, where the 8 is called the units or ones digit, the 7 is called the tens digit, and the 4 is called the hundreds digit. For the rest of this section, we will denote the units digit as a_0, the tens digit as a_1, and so on. Essentially, if we have an n-digit number, then it can be written as

$$\sum_{i=0}^{n-1} 10^i a_i,$$

where $0 \le a_i \le 9$, for all i.

Recall that if a number k is divisible by n, then we can write $k \equiv 0 \pmod{n}$. We will prove most of our divisibility rules this way.

Example 18.26 (Divisibility rule for 3)**.** Prove that if the sum of the digits of a number is divisible by 3, then the original number is also divisible by 3.

Solution. You probably learned this fact in elementary or middle school, but now, it's time to prove it. Let this number have n digits, so we can write it as

$$n = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10^1 a_1 + 10^0 a_0.$$

Now, notice that $10 \equiv 1 \pmod{3} \implies 10^k \equiv 1 \pmod{3}$. Taking n modulo 3 gives us

$$10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10^1 a_1 + 10^0 a_0 \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod{3}.$$

The RHS of the congruence is just the sum of the digits! In the problem statement, we're given that the sum of the digits is divisible by 3, so we know $a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \equiv 0 \pmod{3} \implies 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10^1 a_1 + 10^0 a_0 \equiv n \equiv 0 \pmod{3}$. ■

The divisibility rule for 9 follows a similar argument.

Exercise 18.27. Prove the divisibility rule for 9: If the sum of the digits of a number is divisible by 9, then the original number is also divisible by 9.

Example 18.28 (Divisibility rule for powers of 2)**.** Prove that a number is divisible by 2^k if the number formed by its k rightmost digits are divisible by 2^k, where k is a positive integer.

Solution. You might know the divisibility rule for 4: If the number formed by the last two digits of a number is divisible by 4, then the original number is divisible by 4. The divisibility rule for 8 is similar: If the number formed by the last three digits of a number is divisible by 8,

then the original number is divisible by 8. Let's prove this generalized rule. Suppose we have an $n > k$-digit number. We can write out the base 10 expansion as in the previous example, while noting that $10 = 5 \cdot 2$:

$$\begin{aligned} &10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10^1 a_1 + 10^0 a_0 \\ \equiv\ &2^{n-1}5^{n-1}a_{n-1} + 2^{n-2}5^{n-2}a_{n-2} + \cdots + 2^1 5^1 a_1 + 2^0 5^0 a_0 \pmod{2^k}. \end{aligned}$$

Since we're taking this modulo 2^k, we see that for any value of $l \geq k$, it follows that $2^l \equiv 0 \pmod{2^k}$. Therefore, we can chop off a bunch of digits, until we're left with the k rightmost digits, because those are the only ones that are not congruent to 0 modulo 2^k. Continuing, we get

$$\begin{aligned} &2^{n-1}5^{n-1}a_{n-1} + 2^{n-2}5^{n-2}a_{n-2} + \cdots + 2^1 5^1 a_1 + 2^0 5^0 a_0 \\ \equiv\ &2^{k-1}5^{k-1}a_{k-1} + 2^{k-2}5^{k-2}a_{k-2} + \cdots + 2^1 5^1 a_1 + 2^0 5^0 a_0 \\ \equiv\ &10^{k-1}a_{k-1} + 10^{k-2}a_{k-2} + \cdots 10^1 a_1 + 10^0 a_0 \pmod{2^k}. \end{aligned}$$

Thus, n is congruent to the number formed by the last k digits of n, modulo 2^k. ■

Exercise 18.29. Prove the divisibility rule for 11: Starting from the leftmost digit, add and subtract digits in an alternating manner, until you get to the end. If that sum is divisible by 11, then so is the original number.

§18.4 Challenging examples

Example 18.30 (AoPS). Given that $p \geq 7$ is a prime number, evaluate

$$1^{-1} \cdot 2^{-1} + 2^{-1} \cdot 3^{-1} + 3^{-1} \cdot 4^{-1} + \cdots + (p-2)^{-1} \cdot (p-1)^{-1} \pmod{p}.$$

Solution. First off, we can be sure that all integers between 1 and $p-1$, inclusive, have an inverse, because p is prime. Because modular arithmetic and solving regular equations are so similar, we might look to regular equations for help. If we were just solving a regular sum, then we would have

$$\begin{aligned} &1^{-1} \cdot 2^{-1} + 2^{-1} \cdot 3^{-1} + 3^{-1} \cdot 4^{-1} + \cdots + (p-2)^{-1} \cdot (p-1)^{-1} \\ &\qquad = \frac{1}{1} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{3} + \frac{1}{3} \cdot \frac{1}{4} + \cdots + \frac{1}{p-2} \cdot \frac{1}{p-1}. \end{aligned}$$

Recall that $\frac{1}{n} \cdot \frac{1}{n+1} = \frac{1}{n} - \frac{1}{n+1}$, so we can get a telescoping sum. Let's see if we can achieve the same thing in modular arithmetic. In other words, can we prove that

$$n^{-1} \cdot (n+1)^{-1} \equiv n^{-1} - (n+1)^{-1} \pmod{p}?$$

Multiplying both sides by $n(n+1)$ lets us cancel out some things, by the definition of inverse. We do that, to get

$$\begin{aligned} n^{-1}(n+1)^{-1}n(n+1) &\equiv (n^{-1} - (n+1)^{-1})(n(n+1)) \pmod{p} \\ \implies 1 \equiv n+1-n \pmod{p} &\implies 1 \equiv 1 \pmod{p}. \end{aligned}$$

We've proven that this fact also holds modulo p. This gives us a nice telescoping sum to work with! Continuing, we can see that

$$\begin{aligned} 1^{-1} \cdot 2^{-1} &\equiv 1^{-1} - 2^{-1}, \\ 2^{-1} \cdot 3^{-1} &\equiv 2^{-1} - 3^{-1}, \\ 3^{-1} \cdot 4^{-1} &\equiv 3^{-1} - 4^{-1}, \end{aligned}$$

and so on. Our sum becomes $1^{-1} - 2^{-1} + 2^{-1} - 3^{-1} + 3^{-1} - 4^{-1} + \cdots + (p-2)^{-1} - (p-1)^{-1} \equiv 1^{-1} - (p-1)^{-1} \equiv 1 - (-1) \equiv \boxed{2} \pmod{p}$. ■

Example 18.31 (2014 AIME I)**.** The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

Solution. If N and N^2 have the same last 4 digits, then we can say that

$$N^2 \equiv N \pmod{10^4} \implies N(N-1) \equiv 0 \pmod{10^4}. \tag{18.1}$$

We also know that $a \neq 0$, so N is at least a 4-digit number. Finally, N can't be something along the lines of 10000, because that also clearly violates our $a \neq 0$ condition.

From (5.1), we can see that $N(N-1)$ must be a multiple of $10^4 = 2^4 \cdot 5^4$. Furthermore, one of $N,\ N-1$ must be a multiple of 5^4 but not divisible by 2, and the other one must be a multiple of 2^4 but not divisible by 5 (do a proof by contradiction to see why; what happens when one of $N,\ N-1$ is a multiple of both 2 and 5?).

Let's use the fact that one of $N,\ N-1$ is an odd multiple of $5^4 = 625$. We can write this number as $625 + 2 \cdot 625 \cdot k = 625 + 1250k$, for some positive integer k.

If $N = 625 + 1250k$, then $N - 1$ must be divisible by 16. We can write

$$N - 1 \equiv 0 \pmod{16} \implies 625 + 1250k \equiv 1 \pmod{16}.$$

If $N - 1 = 625 + 1250k$, then N must be divisible by 16, and we can write

$$N \equiv 0 \pmod{16} \implies N - 1 \equiv -1 \pmod{16} \implies 625 + 1250k \equiv -1 \pmod{16}.$$

Combining, we see that we must find a k such that

$$625 + 1250k \equiv \pm 1 \pmod{16}.$$

Continuing, we have $625 \equiv 1 \pmod{16} \implies 1250 \equiv 2 \cdot 625 \equiv 2 \pmod{16} \implies 625 + 1250k \equiv 1 + 2k \pmod{16}$. An obvious value of k that would make the congruence equivalent to ± 1 modulo 16 would be $k = 0$. However, we would get $N = 625$ and $N - 1 = 624$, which, although N and N^2 do end in the same 4 digits, does not satisfy our given restriction of $a \neq 0$.

The next smallest possible value of k would be

$$k = 7 \implies 1 + 2k \equiv -1 \pmod{16} \implies N - 1 = 9375,\ N = 9376.$$

This satisfies our condition on a not being 0. Therefore, our answer is $\boxed{937}$. Indeed, $N = 9376$ and $N^2 = 87909376$. ■

Example 18.32 (2011 AIME I). Find the number of positive integers m for which there exist nonnegative integers x_0, x_1 , … , x_{2011} such that

$$m^{x_0} = \sum_{k=1}^{2011} m^{x_k}.$$

Solution. This problem just spits out a bunch of symbols, so let's try to make sense of this. It wants us to find how many positive integer values of m there are such that m to some power can be written as the sum of 2011 not necessarily distinct powers of m.

Let's begin by taking both sides modulo $m-1$. Note that $m \equiv 1 \pmod{m-1}$, so the LHS reduces nicely to $m^{x_0} \equiv 1^{x_0} \equiv 1 \pmod{m-1}$, and the RHS reduces to

$$\sum_{k=1}^{2011} m^{x_k} \equiv \sum_{k=1}^{2011} 1^{x_k} \equiv 2011 \pmod{m-1}.$$

Setting the LHS congruent to the RHS, we get

$$1 \equiv 2011 \pmod{m-1} \implies 2010 \equiv 0 \pmod{m-1}.$$

This tells us that $m-1$ must be a factor of 2010. Now, we have to make sure that all values of m, for which $m-1$ is a factor of 2010, are achievable. In other words, we're still not sure if this condition is our tightest restriction, but let's try to prove that it is. The smallest possible value for m is 2, because $2-1=1$ is a factor of 2010. Let's try to find $x_0, x_1, \ldots, x_{2011}$ such that

$$2^{x_0} = \sum_{k=1}^{2011} 2^{x_k}.$$

Note that if we have $x_0 = 2010$, then on the RHS, we can have the sum $2^0+2^0+2^1+2^2+\cdots+2^{2009}$, and it satisfies the equation.

We can do a similar thing for $m=3$. On the RHS, we can have the sum $3^0+3^0+3^0+3^1+3^1+3^2+3^2+\cdots+3^{1004}+3^{1004}$ (check if this sum has exactly 2011 terms), which sums up to 3^{1005}.

In general, we can construct a power of m using 2011 powers of m by having

$$\underbrace{m^0+m^0+\cdots+m^0}_{m \text{ terms}} + \underbrace{m^1+m^1+\cdots+m^1}_{m-1 \text{ terms}} + \cdots + \underbrace{m^k+m^k+\cdots+m^k}_{m-1 \text{ terms}} = m^{k+1},$$

where k is some positive integer (in the case of $m=2$, $k=2009$, and in the case of $m=3$, $k=1004$. What matters is that k changes as m changes). Lastly, we need to verify that this sum has exactly 2011 terms whenever $m-1$ is a factor of 2010. Sure enough, we can count the number of terms. Looking back at our sum, we have

$$\underbrace{m^0+m^0+\cdots+m^0}_{m \text{ terms}} + \underbrace{\underbrace{m^1+m^1+\cdots+m^1}_{m-1 \text{ terms}} + \cdots + \underbrace{m^k+m^k+\cdots+m^k}_{m-1 \text{ terms}}}_{k \text{ of these}} = m^{k+1}.$$

Therefore, the number of terms is

$$m + \underbrace{(m-1)+(m-1)+\cdots+(m-1)}_{k \text{ of these}} = m + k(m-1) = m-1+1+k(m-1)$$

$$= (k+1)(m-1)+1 = 2011 \implies (k+1)(m-1) = 2010.$$

Hence, $m-1$ must be a factor of 2010, since we have defined k to be an integer. We have shown that this way of constructing a power of m works for all m with $m-1|2010$, so all that's left to do is find how many values of m satisfy $m-1|2010$. This is simply equal to $\tau(2010) = \tau(2 \cdot 3 \cdot 5 \cdot 67) = \boxed{016}$. ■

§18.5 Homework Problems

Problem 18.1. [3] How many positive integers $n \leq 2020$ are there such that $2^n + 1$ is divisible by 3?

Problem 18.2. [3] Find the remainder when 20^{20} is divided by 13.

Problem 18.3 (Dennis Chen)**.** [4] How many integers x with $1 \leq x \leq 100$ are there such that $x^2 + 8x + 15$ is divisible by 10?

Problem 18.4 (AoPS)**.** [4] What is the smallest positive integer a such that a^{-1} is undefined (mod 55) and a^{-1} is also undefined (mod 66)?

Problem 18.5. [4] What is the remainder when

$$\sum_{n=1}^{2020} n \cdot 20^n$$

is divided by 19?

Problem 18.6 (2017 AMC 12)**.** [5] Claire adds the degree measures of the interior angles of a convex polygon and arrives at a sum of 2017. She then discovers that she forgot to include one angle. What is the degree measure of the forgotten angle?

Problem 18.7 (2010 AIME I)**.** [5] Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$ is divided by 1000.

Problem 18.8 (2018 AMC 10B)**.** [5] Let $a_1, a_2, \ldots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$

What is the remainder when $a_1^3 + a_2^3 + \cdots + a_{2018}^3$ is divided by 6?

Problem 18.9 (2017 AIME II)**.** [9] Find the number of positive integers n less than 2017 such that

$$1 + n + \frac{n^2}{2!} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!}$$

is an integer.

Problem 18.10 (2003 AMC 10)**.** [7] Let n be a 5-digit number, and let q and r be the quotient and the remainder, respectively, when n is divided by 100. For how many values of n is $q + r$ divisible by 11?

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

19 Chinese Remainder Theorem, Fermat's Little Theorem, and Euler's Theorem

In this handout, we'll go over some more advanced techniques relating to modular arithmetic.

§19.1 The Chinese Remainder Theorem

You might remember being introduced to the methods of substitution and elimination to solve a system of equations. Analogously, the Chinese Remainder Theorem is used to solve a system of linear congruences.

Example 19.1. Find the smallest positive integer solution for x given that it satisfies $2x \equiv 7 \pmod{11}$ and $5x \equiv 1 \pmod{3}$.

Solution. We should begin by solving each congruence for x. The first congruence requires us to find the inverse of 2 modulo 11. Since $2 \cdot 6 \equiv 12 \equiv 1 \pmod{11}$, we know that $2^{-1} \equiv 6 \pmod{11}$. It follows that

$$2x \equiv 7 \pmod{11} \implies x \equiv 7 \cdot 2^{-1} \equiv 7 \cdot 6 \equiv 42 \equiv 9 \pmod{11}.$$

For the second congruence, we can already reduce it down:

$$5x \equiv 1 \pmod{3} \implies 2x \equiv 1 \pmod{3} \implies x \equiv 2^{-1} \pmod{3}.$$

We know that $2 \equiv -1 \pmod{3}$. Since $(-1)(-1) \equiv 1 \pmod{3}$, then we can replace the -1s with 2s, and get that 2 is its own inverse modulo 3. Thus,

$$x \equiv 2^{-1} \equiv 2 \pmod{3}.$$

Then, we list out the first few positive integers that are congruent to 9 modulo 11: 9, 20, 31, ... We see that 20 is also congruent to 2 modulo 3, so our answer is $\boxed{20}$. ■

That was pretty unsatisfying. What would we do if we had bigger numbers? We just kind of guessed and checked our way through the problem, and it worked, simply because the numbers were manageable.

To generalize the idea of constructing a solution to a system of modular equations, we introduce the Chinese Remainder Theorem (CRT):

Theorem 19.2 (Chinese Remainder Theorem). *If $b_1, b_2, \ldots, b_r$ are pairwise relatively prime positive integers, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{b_1} \\ x &\equiv a_2 \pmod{b_2} \\ &\vdots \\ x &\equiv a_r \pmod{b_r} \end{aligned}$$

has a unique solution for x modulo $b_1 b_2 \cdots b_r$.
In particular, the solution for x is constructed as follows: Let $B = b_1 b_2 \cdots b_r$ and let $B_i = B/b_i$, for all i, with $1 \leq i \leq r$. Let $c_i \equiv B_i^{-1} \pmod{b_i}$. In other words, c_i is the inverse of B_i, mod b_i. Then,

$$x \equiv \sum_{i=1}^{r} a_i B_i c_i \equiv a_1 B_1 c_1 + a_2 B_2 c_2 + \cdots + a_r B_r c_r \pmod{B}.$$

Proof. We prove that the solution for x is unique. We first prove the following general statement:

If

$$\begin{aligned} x &\equiv y \pmod{b_1} \\ x &\equiv y \pmod{b_2} \\ &\vdots \\ x &\equiv y \pmod{b_r}, \end{aligned}$$

then $x \equiv y \pmod{\operatorname{lcm}(b_1, b_2, \ldots, b_r)}$.

We can rearrange the congruences to get

$$\begin{aligned} x - y &\equiv 0 \pmod{b_1} \\ x - y &\equiv 0 \pmod{b_2} \\ &\vdots \\ x - y &\equiv 0 \pmod{b_r}. \end{aligned}$$

It follows that $b_1 | (x-y),\ b_2 | (x-y), \ldots, b_r | (x-y)$. Recall that if for positive integers a, b, and c, we have $a|c$ and $b|c$, then $\operatorname{lcm}(a,b)|c$.

Therefore,

$$\operatorname{lcm}(b_1, b_2, \ldots, b_r) | (x-y) \implies x \equiv y \pmod{\operatorname{lcm}(b_1, b_2, \ldots, b_r)}.$$

An immediate corollary to this is when $b_1, b_2, \ldots, b_r$ are pairwise relatively prime. This means that $\operatorname{lcm}(b_1, b_2, \ldots, b_r) = b_1 b_2 \cdots b_r \implies x \equiv y \pmod{b_1 b_2 \cdots b_r}$.

Now, we turn our eyes back to the CRT. Suppose that x_1 and x_2 are both solutions to the following system of congruences for x :

$$\begin{aligned} x &\equiv a_1 \pmod{b_1} \\ x &\equiv a_2 \pmod{b_2} \\ &\vdots \\ x &\equiv a_r \pmod{b_r}, \end{aligned}$$

where $b_1, b_2, \ldots, b_r$ are pairwise relatively prime. It follows that $x_1 \equiv x_2 \equiv a_i \pmod{b_i}$ for all i between 1 and r, inclusive. From what we proved earlier, we have

$$x_1 \equiv x_2 \pmod{b_1 b_2 \cdots b_r},$$

so the solution of the system is unique modulo $b_1 b_2 \cdots b_r$. ■

Existence of the solution is already given by our construction in the theorem statement. We'll verify it now.

Example 19.3. Verify that the given solution for x in the theorem satisfies all of the congruences.

Solution. To get an idea of what we're working with, let's take the sum modulo b_1. Since $B_2 = b_1 b_3 b_4 \cdots b_r$, then we know that $B_2 \equiv 0 \pmod{b_1}$. Also, $B_3 = b_1 b_2 b_4 b_5 \cdots b_r$, then we know that $B_3 \equiv 0 \pmod{b_1}$ as well. In fact, $B_j \equiv 0 \pmod{b_1}$ for all $j \neq 1$, because b_1 will always be a factor. Thus,

$$a_1 B_1 c_1 + a_2 B_2 c_2 + \cdots + a_r B_r c_r \equiv a_1 B_1 c_1 \pmod{b_1}.$$

By the definition of c_i, we know that c_1 is the inverse of B_1 modulo b_1. In other words, we can write $c_1 B_1 \equiv 1 \pmod{b_1}$. Therefore,

$$a_1 B_1 c_1 \equiv a_1 \cdot 1 \equiv a_1 \pmod{b_1},$$

so x satisfies the first congruence. Now, we prove that $x \equiv a_k \pmod{b_k}$, for all k between 2 and r, inclusive.

Notice that $b_k | B_j$ for all $j \neq k$. Hence,

$$a_1 B_1 c_1 + a_2 B_2 c_2 + \cdots + a_r B_r c_r \equiv a_k B_k c_k \pmod{b_k}.$$

Recall that $B_k c_k \equiv 1 \pmod{b_k}$ for all k, so

$$a_k B_k c_k \equiv a_k \pmod{b_k},$$

as desired. ■

Remark. Don't memorize this long statement! It's more important to know how the formula works. The most important thing for you is to see how we used inverses and divisibility to force a sum to satisfy many different congruences at once.

Example 19.4. Solve the system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \end{aligned}$$

Solution. We use the Chinese Remainder Theorem to solve this. Afterwards, we will show another way to solve systems of congruences, called back-substitution.

Be careful! In order to use CRT, then we have to make sure that all of our moduli are pairwise congruent. For this problem, we're good, since we're using only primes. Now, we compute

$$B = 3 \cdot 5 \cdot 7 = 105 \implies B_1 = 35, B_2 = 21, B_3 = 15.$$

We work term by term. We must make sure that the first term in the sum is congruent to 1 mod 3. Therefore,

$$B_1 c_1 \equiv 35 \cdot c_1 \equiv 1 \pmod{3} \implies c_1 = 2.$$

Similarly,

$$B_2c_2 \equiv 21 \cdot c_2 \equiv 1 \pmod 5 \implies c_2 = 1,$$
$$B_3c_3 \equiv 15 \cdot c_3 \equiv 1 \pmod 7 \implies c_3 = 1.$$

Thus, $x \equiv 1 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 \equiv 208 \equiv \boxed{103 \pmod{105}}$. ■

Solution. For this solution, we build up using "back-substitution". Since $x \equiv 1 \pmod 3$, then recall that we can write $x = 3q + 1$, for some integer q. Substituting this into our second congruence, we get

$$x \equiv 3 \pmod 5 \implies 3q + 1 \equiv 3 \pmod 5 \implies q \equiv 4 \pmod 5.$$

Thus, we write $q = 5r + 4$, for some integer r. Back-substituting, we have $x = 3q + 1 = 3(5r + 4) + 1 = 15r + 13$. Now, we use our last congruence:

$$x \equiv 5 \pmod 7 \implies 15r + 13 \equiv 5 \pmod 7 \implies r \equiv 6 \pmod 7 \implies r = 7s + 6,$$

for some integer s. Back-substituting again, we arrive at

$$x = 15r + 13 = 15(7s + 6) + 13 = 105s + 103 \implies \boxed{x \equiv 103 \pmod{105}}.$$

■

Solution. There is a slicker solution, that actually doesn't involve any advanced method. Observe that we can rewrite the congruences as

$$x \equiv -2 \pmod 3$$
$$x \equiv -2 \pmod 5$$
$$x \equiv -2 \pmod 7.$$

Using the ideas discussed in the proof of the uniqueness of the solution in CRT, we have that $x + 2$ is a multiple of 3, 5, and 7. It follows that

$$x + 2 \equiv 0 \pmod{3 \cdot 5 \cdot 7} \implies \boxed{x \equiv 103 \pmod{105}}.$$

■

Example 19.5. The students in a classroom are arranged in a rectangular formation. When they are arranged in 9 rows, there are 3 positions unoccupied. When they are arranged in 11 rows, there is 1 position unoccupied. How many students are in the class if the class size is between 100 and 200?

Solution. Let n be the number of students in the class. We can write a system of modular congruences to model this problem.

$$n \equiv -3 \pmod 9$$
$$n \equiv -1 \pmod{11}$$

This is equivalent to the following:

$$n \equiv 6 \pmod 9$$
$$n \equiv 10 \pmod{11}$$

Using the Euclidean Algorithm, we find that the inverse of 9 mod 11 is 5 and the inverse of 11 mod 9 is 5. Therefore, using our earlier summation formula, we have $n = 6(11)(5) + 10(9)(5) = 780 \equiv 87 \pmod{99}$. The problem states that $100 \leq n \leq 200$, so the answer is $87 + 99 = \boxed{186}$. ■

Example 19.6. Show that there exists a multiple of 2013 whose last four digits are 2014.

Solution. At first glance, this number, which we can call X, seems really big. However, we don't actually need to find this number, we simply need to show that it exists.

Recall that the core idea of CRT is that a system of congruences with pairwise coprime moduli always has a solution. Once we construct a system of congruences that satisfies the problem's constraints, we're done, by CRT. From the first part of the problem statement, we have

$$X \equiv 0 \pmod{2013}.$$

We're also given that the last four digits of X are 2014, so we can write

$$X \equiv 2014 \pmod{10000}.$$

Since $\gcd(2013, 10000) = 1$, CRT applies, and it tells us that there exists a solution. ■

Example 19.7. Find the last three digits of $124^{2020} + 2020$ without a calculator.

Solution. For the sake of brevity, let's say that $N = 124^{2020} + 2020$. Finding the last three digits of N is equivalent to finding the remainder when N is divided by 1000. In other words, we want to reduce N down modulo 1000.

It would be really hard to do this without a calculator, so we look to a new strategy. We want to split up the problem into smaller moduli so that we can use CRT. This means that we need to find b_1 and b_2 such that $\gcd(b_1, b_2) = 1$ and $b_1 b_2 = 1000$. The only pair that works is $b_1 = 8, b_2 = 125$.

Our new idea is this: We want to solve the following system of congruences for N:

$$\begin{aligned} N &\equiv l_1 \pmod{8} \\ N &\equiv l_2 \pmod{125}, \end{aligned}$$

where l_1 is the least residue of N modulo 8 and l_2 is the least residue of N modulo 125. To proceed, we need to find l_1 and l_2. Since $124^{2020} = 4^{2020}31^{2020}$ is clearly divisible by 8, we have

$$124^{2020} \equiv 0 \pmod{8} \implies 124^{2020} + 2020 \equiv 2020 \equiv 4 \pmod{8} \implies l_1 = 4.$$

For modulo 125, we use the fact that $124 \equiv -1 \pmod{125}$, to get

$$124^{2020} \equiv (-1)^{2020} \equiv 1 \implies N \equiv 1 + 2020 \equiv 21 \pmod{125} \implies l_2 = 21.$$

Thus, our system of congruences that we want to solve is

$$\begin{aligned} N &\equiv 4 \pmod{8} \\ N &\equiv 21 \pmod{125}. \end{aligned}$$

Since we only have two congruences, we back-substitute instead of breaking out the CRT sum formula. From the first congruence, we can write $x = 8q + 4$, for some integer q. Then, our second congruence becomes $8q + 4 \equiv 21 \pmod{125} \implies 8q \equiv 17 \pmod{125}$. Ooh, this is a bit tough to solve, since our modulus is so big. Let's go the other way around and start with the second congruence.

We have $N = 125q + 21$, for some integer q. Then, we substitute this in for N in our first congruence, to get

$$125q + 21 \equiv 4 \pmod{8} \implies 5q + 5 \equiv 4 \pmod{8} \implies q \equiv 3 \pmod{8}.$$

We can write $q = 8r + 3$, for some integer r, which gives us

$$N = 125q + 21 = 125(8r + 3) + 21 = 1000r + 375 + 21 = 1000r + 396.$$

Therefore, the last three digits of N are $\boxed{396}$. ■

> *Remark.* No one likes big numbers. We like working with small moduli, so we reduced the problem down until the size of the moduli was manageable.

If the number didn't involve 124 to some power and instead involved, say, 97 to some power, then we would have had a much harder time reducing it modulo 125. Do not worry! FLT and Euler's Theorem are both very helpful in this regard.

§19.1.1 Exercises for this section

Exercise 19.8. Solve the following system of congruences for x :

$$\begin{aligned} x &\equiv 19 \pmod{21} \\ x &\equiv 15 \pmod{20} \\ x &\equiv 11 \pmod{19}. \end{aligned}$$

Exercise 19.9. Show that there exists a multiple of 2019 that is 1 more than a multiple of 2020.

Exercise 19.10. Find the smallest positive integer solution for x if

$$\begin{aligned} 2x &\equiv 4 \pmod{6} \\ 3x &\equiv 6 \pmod{25} \\ 3x &\equiv 8 \pmod{21} \\ 5x &\equiv 10 \pmod{11}. \end{aligned}$$

Hint: What needs to be true in order for CRT to work?

§19.2 Fermat's Little Theorem

The remaining sections are very important, because they contain methods to reduce large numbers. These theorems are worth memorizing. We start off this section with another theorem: Wilson's Theorem. This will help us in our proof of FLT.

Example 19.11. Find the remainder when 10! is divided by 11.

Solution. Don't bash it out! Let's use inverses to solve this. Note that

$$\begin{aligned} 2^{-1} &\equiv 6 \pmod{11} \\ 3^{-1} &\equiv 4 \pmod{11} \\ 5^{-1} &\equiv 9 \pmod{11} \\ 7^{-1} &\equiv 8 \pmod{11}. \end{aligned}$$

Thus,

$$10! \equiv 1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 \equiv 10 \pmod{11},$$

and the remainder is $\boxed{10}$. ■

Theorem 19.12 (Wilson's Theorem). *If p is a prime number, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Similar to the example above, we use inverses. In Example 5.13 from the previous handout, we proved that the only time when a is its own inverse modulo p, where p is a prime, is when $a \equiv -1$ or $1 \pmod{p}$. For this proof, we assume that $p \geq 5$ (it is easy to see that $p = 2$ and $p = 3$ work).

Remark that $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1)$ and consider the product $2 \cdot 3 \cdots (p-3)(p-2)$. Recall that the inverse of a is unique modulo p, which implies that we can group the set of numbers $\{2, 3, \ldots, p-3, p-2\}$ into pairs of inverses modulo p.

For instance, in the previous example, the pairs would be $(2, 6), (3, 4), (5, 9)$, and $(7, 8)$. We can be sure that all our pairs are disjoint, meaning no two pairs share a common number, because of the uniqueness property.

Why did we pair up numbers like this? So that we can use inverses! The product of the two numbers in every pair is congruent to 1 modulo p, so we have

$$2 \cdot 3 \cdots (p-3)(p-2) \equiv 1 \pmod{p} \implies (p-1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

■

Now, we can move on to FLT. We first illustrate how Fermat's Little Theorem is useful with an example.

Example 19.13 (MATHCOUNTS). Find the remainder when 11^{12} is divided by 13.

Solution. We want to find the least residue of 11^{12} modulo 13. Note that $11 \equiv -2 \pmod{13}$, so we have

$$11^{12} \equiv (-2)^{12} \equiv 2^6 \cdot 2^6 \equiv 64 \cdot 64 \equiv (-1)(-1) \equiv 1 \pmod{13},$$

so our answer is $\boxed{1}$. ■

That took a bit of work, and without prior knowledge of modular arithmetic, would've taken longer. However, FLT completely trivializes this problem.

Theorem 19.14 (Fermat's Little Theorem). *If p is a prime number, and a is a positive integer with $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

We present two proofs of FLT: one using Wilson's theorem, and one using induction, in hopes that both will be beneficial.

Proof. Suppose that p is a prime number a is some positive integer such that $p \nmid a$. Then, the elements in the following set:

$$S = \{a, 2a, 3a, \ldots, (p-2)a, (p-1)a\}$$

are pairwise incongruent and hit all possible residues except for 0 modulo p.

We first prove that they are pairwise in congruent. Suppose to the contrary that there exist i, j such that $1 \leq i \neq j \leq p-1$ and $ia \equiv ja \pmod{p}$. Rearranging the congruence gives us

$$ia - ja \equiv 0 \pmod{p} \implies (i-j)a \equiv 0 \pmod{p}.$$

It follows that $i-j$ must be a multiple of p, but $i-j \leq p-1$, so we've arrived at a contradiction.

Note that the possible residues modulo p are $\{0, 1, 2, \ldots, p-2, p-1\}$. S contains $p-1$ elements, which are pairwise incongruent to each other, and none of the elements are congruent to 0 (mod p). This means that the elements in S taken modulo p are a permutation of $\{1, 2, \ldots, p-2, p-1\}$. Thus, if P is the product of all the elements in S, then

$$\begin{aligned} & P \equiv (p-1)! \pmod{p} \\ \implies & a \cdot 2a \cdot 3a \cdots (p-1)a \equiv -1 \pmod{p} \\ \implies & (p-1)! a^{p-1} \equiv -1 \pmod{p} \\ \implies & -a^{p-1} \equiv -1 \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p}. \end{aligned}$$

■

Proof. Our second proof uses induction. Note that

$$a^{p-1} \equiv 1 \pmod{p} \iff a^p \equiv a \pmod{p}.$$

Thus, we want to prove that $a^p \equiv a \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$. It suffices to prove the congruence holds for all a in the range $1 \leq a \leq p-1$.

For our base case, we have $a = 1$. Indeed, $1^p \equiv 1 \pmod{p}$.

For the inductive step, we assume that $a^p \equiv a \pmod{p}$ for some a between 1 and $p-2$. We seek to prove that $(a+1)^p \equiv a+1 \pmod{p}$ as well. Indeed, by the binomial theorem,

$$(a+1)^p \equiv a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a^1 + 1 \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

Thus, $a^p \equiv a \pmod{p}$ for all a between 1 and $p-1$, inclusive. If instead we have $a > p$, then a will still be congruent to some integer between 1 and $p-1$, because $p \nmid a$, so our conclusion holds for all positive a that is not divisible by p. ■

Example 19.15 (2008 AMC 12). Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

Solution. If we want the units digit, we think of the problem modulo 10. However, reducing the 2^{2008} looks nasty, and FLT requires the modulus to be prime, so we split up the problem into mod 2 and mod 5, then use CRT. We find $k^2 + 2^k$ modulo 2 first. Note that k is even, so

$$k^2 + 2^k \equiv 0 + 0 \equiv 0 \pmod 2.$$

For modulo 5, we use FLT to reduce k. In particular, it tells us that $2^{5-1} \equiv 1 \pmod 5$. Therefore,

$$2008^2 + 2^{2008} \equiv 3^2 + \left(2^4\right)^{502} \equiv 9 + 1 \equiv 0 \pmod 5 \implies k^2 \equiv 0 \pmod 5.$$

To find 2^k modulo 5, we need to find k modulo 4. To see why, simply let $k = 4q + r$, where r is the remainder when k is divided by 4. Then, we have

$$2^k \equiv 2^{4q+r} \equiv \underbrace{2^4 2^4 2^4 \cdots 2^4}_{q \text{ of these}} \cdot 2^r \equiv 2^r \pmod 5.$$

Note that $4|2008^2$ and $4|2^{2008}$, so $k \equiv 0 \pmod 4 \implies r = 0 \implies 2^k \equiv 2^r \equiv 1 \pmod 5 \implies k^2 + 2^k \equiv 1 \pmod 5$. Thus, we have the following system of congruences:

$$\begin{aligned} k^2 + 2^k &\equiv 0 \pmod 2 \\ k^2 + 2^k &\equiv 1 \pmod 5. \end{aligned}$$

It follows that $k^2 + 2^k \equiv 6 \pmod{10}$, so the units digit is $\boxed{6}$. ■

Remark. If a and n are relatively prime positive integers such that $a^x \equiv 1 \pmod n$ and $y > x$, then $a^y \equiv a^r \pmod n$, where r is the remainder when y is divided by x. We will use this idea a lot in the next section.

Exercises for this section:

Exercise 19.16 (AoPS). Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod 7$.

Exercise 19.17. Find all n such that $5^n - 4^n$ is divisible by 61.

Exercise 19.18. The **order** of a modulo n is the smallest positive integer r such that $a^r \equiv 1 \pmod n$. If n is a prime and a is a positive integer that does not divide n, then is the order of a always $n - 1$? Find two values of a and n for which the order is $n - 1$ and two values of when it is not.

Exercise 19.19. Prove the converse of Wilson's Theorem: If $(p-1)! \equiv -1 \pmod p$, then p is a prime number. **Hint:** Do a proof by contradiction: assume that p is composite.

§19.3 Euler's Theorem

What if the modulus isn't prime? FLT only deals with prime moduli, after all. Euler's theorem generalizes this to all moduli.

Theorem 19.20 (Euler's Theorem). *If* $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

where $\phi(n)$ *is the number of positive integers less than or equal to* n *that are relatively prime to* n.

Proof. This proof will be very similar to the proof for FLT. We define a *reduced residue system* (RRS) modulo n to be a set of $\phi(n)$ numbers such that every integer relatively prime to n is congruent to some element in the set. For example, the following sets would be RRS's modulo 10:

$$\{1, 3, 7, 9\},\ \{11, 13, 17, 19\},\ \{-19, 1113, 917, 9\}$$

and these sets would not be RRS's modulo 10:

$$\{2, 4, 6, 9\},\ \{1, 2, 3, 4, \ldots, 9, 10\},\ \{1, 3, 5, 7\}.$$

Recall that in the proof of FLT, we showed that $\{a, 2a, 3a, \ldots, (p-2)a, (p-1)a\}$ was a permutation of $\{1, 2, 3, \ldots, p-2, p-1\}$, modulo p. It turns out that the same thing holds for a RRS! Let

$$S = \{r_1, r_2, \ldots, r_{\phi(n)-1}, r_{\phi(n)}\}$$

be the set of positive integers less than n that are relatively prime to n. Note that it is a RRS, modulo n. Then, for any a such that $\gcd(a, n) = 1$, the set

$$S' = \{ar_1, ar_2, \ldots, ar_{\phi(n)-1}, ar_{\phi(n)}\}$$

is also a RRS. To show this, we want to show that all of the elements in S' are relatively prime to n, and that the elements are pairwise relatively prime. We will use proof by contradiction to prove both of these facts.

To prove that all of the elements are in S' are relatively prime to n, we suppose to the contrary that there exists i between 1 and $\phi(n)$, inclusive, such that $\gcd(ar_i, n) > 1$. This tells us that either $\gcd(a, n) > 1$ or $\gcd(r_i, n) > 1$. We defined a to be relatively prime to n, and r_i was also defined to be part of a reduced residue system, so we know that $\gcd(r_i, n) = 1$. Thus, we have arrived at a contradiction.

To prove that all the elements in S' are pairwise relatively prime, we suppose to the contrary that there exist i, j, where $1 \leq i \neq j \leq \phi(n)$, such that

$$ar_i \equiv ar_j \pmod{n} \implies a(r_i - r_j) \equiv 0 \pmod{n}.$$

Hence, one of $a, r_i - r_j$ must be a multiple of n. However, $\gcd(a, n) = 1$, so we must have $r_i - r_j$ be a multiple of n. However, we defined S to only contain elements that are positive and less than n, so $r_i - r_j < n$. Thus, we have arrived at another contradiction, meaning that we've proved that

$$\{ar_1, ar_2, \ldots, ar_{\phi(n)-1}, ar_{\phi(n)}\}$$

is a RRS. To finish, we take the product of all elements in S and all elements in S', and set them to be congruent to each other:

$$\begin{aligned} r_1 r_2 \cdots r_{\phi(n)-1} r_{\phi(n)} &\equiv a r_1 a r_2 \cdots a r_{\phi(n)-1} a r_{\phi(n)} \pmod{n} \\ \implies r_1 r_2 \cdots r_{\phi(n)-1} r_{\phi(n)} &\equiv r_1 r_2 \cdots r_{\phi(n)-1} r_{\phi(n)} a^{\phi(n)} \pmod{n}. \end{aligned}$$

We can divide both sides by $r_1 r_2 \cdots r_{\phi(n)-1} r_{\phi(n)}$, since we know that $\gcd(r_1 r_2 \cdots r_{\phi(n)-1} r_{\phi(n)}, n) = 1$. Doing so gives us

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

■

Anyways, recall that if $n = {p_1}^{k_1} {p_2}^{k_2} \ldots {p_m}^{k_m}$, then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Note that if n is a prime number, then $\phi(n) = n - 1$. By Euler's Theorem,

$$a^{\phi(n)} \equiv a^{n-1} \equiv 1 \pmod{n},$$

which is just FLT! Hence, we say that Euler's Theorem is a generalization of FLT. Euler's Theorem also gives us a reliable way to find inverses, besides using the Euclidean Algorithm:

Proposition 19.21. *If* $\gcd(a, n) = 1$, *then*

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n}.$$

Proof. By Euler's, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$. Recall that $a \cdot a^{-1} \equiv 1 \pmod{n}$, so it follows that $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$. ■

Now let's do some examples to better understand how to use Euler's Theorem.

Example 19.22. Find the remainder when $2019^{2020^{2021}}$ is divided by 1000.

Solution. As usual, we split the problem up into mod 8 and mod 125 to downsize our numbers. Let $N = 2019^{2020^{2021}}$, for shortness. First, we want to find N modulo 8. By Euler's, $2019^{\phi(8)} \equiv 1 \pmod{8}$. Computing, we have $\phi(8) = 8\left(1 - \frac{1}{2}\right) = 4 \implies 2019^4 \equiv 1 \pmod{8}$. It follows that

$$2019^{2020^{2021}} \equiv 1 \pmod{8},$$

because 2020^{2021} is divisible by 4.

Now for modulo 125. We use Euler's Theorem again, and note that $\phi(125) = 125\left(1 - \frac{1}{5}\right) = 100$, to get

$$2019^{\phi(125)} \equiv 1 \pmod{125} \implies 2019^{100} \equiv 1 \pmod{125}.$$

Thus, our next step is to find 2020^{2021} modulo 100. We don't have to do Euler's again, because it's easy to see that

$$2020^{2021} = 202^{2021} \cdot 10^{2021},$$

so $2020^{2021} \equiv 0 \pmod{100} \implies 2019^{2020^{2021}} \equiv 1 \pmod{125}$. Combining, we have

$$\begin{aligned} N &\equiv 1 \pmod 8 \\ N &\equiv 1 \pmod{125}, \end{aligned}$$

implying that $N \equiv 1 \pmod{1000}$, so the remainder is $\boxed{1}$. ■

Example 19.23. Find the inverse of 5 modulo 36 using Euler's Theorem.

Solution. We use the fact that $a^{-1} \equiv a^{\phi(n)-1} \pmod{36}$ when $\gcd(a, n) = 1$. Here, we have $\gcd(5, 36) = 1$, so we're good to go. Plugging in the numbers, we see that

$$5^{-1} \equiv 5^{\phi(36)-1} \pmod{36},$$

where $\phi(36) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12$, so we just need to find $5^{\phi(36)-1} = 5^{11} \bmod 36$. This isn't *too* bad as long as we keep the number reasonably small:

$$\begin{aligned} 5^2 &\equiv 25 \pmod{36} \\ 5^3 &\equiv 125 \equiv 17 \pmod{36} \\ 5^6 &\equiv 5^3 5^3 \equiv 17 \cdot 17 \equiv 289 \equiv 1 \pmod{36} \\ 5^{11} &\equiv 5^6 5^3 5^2 \equiv 1 \cdot 17 \cdot 25 \equiv 425 \equiv 29 \pmod{36}. \end{aligned}$$

Hence, $\boxed{5^{-1} \equiv 29 \pmod{36}}$. ■

Let's do a slightly harder example to finish off this section.

Example 19.24 (2011 AMC 10). What is the hundreds digit of 2011^{2011}?

Solution. We essentially want to find $2011^{2011} \bmod 1000$. Before we split up the problem into mod 8 and mod 125, notice that we can already reduce this mod 100, since $2011 \equiv 11 \pmod{1000}$. Now, we split up. We consider 11^{2011} modulo 8 first. We have $11 \equiv 3 \pmod 8$, so

$$11^{2011} \equiv (3)^{2011} \pmod 8.$$

By Euler's, we know that $\phi(8) = 8\left(1 - \frac{1}{2}\right) = 4$, so $3^4 \equiv 1 \pmod 8$. We know that $2011 \equiv 3 \pmod 4$. Hence,

$$3^{2011} \equiv 3^3 \equiv 27 \equiv 3 \pmod 8.$$

For modulo 125, we use Euler's again to get that $11^{\phi(125)} \equiv 1 \pmod{125}$, where $\phi(125) = 125\left(1 - \frac{1}{5}\right) = 100$. It follows that

$$11^{2011} \equiv 11^{11} \pmod{25}.$$

Then, we bash it out:

$$\begin{aligned} 11^2 &\equiv 121 \equiv -4 \pmod{125} \\ 11^4 &\equiv 11^2 11^2 \equiv (-4)(-4) \equiv 16 \pmod{125} \\ 11^8 &\equiv 11^4 11^4 \equiv 16 \cdot 16 \equiv 256 \equiv 6 \pmod{125} \\ 11^{11} &\equiv 11^8 11^2 \cdot 11 \equiv 6 \cdot (-4) \cdot 11 \equiv -264 \equiv -14 \equiv 111 \pmod{125}. \end{aligned}$$

Thus, our system of congruences is

$$11^{2011} \equiv 3 \pmod 8$$
$$11^{2011} \equiv 111 \pmod{125}.$$

We let $11^{2011} = 125q + 111$ for some integer q, then substitute it into the first congruence:

$$11^{2011} \equiv 125q + 111 \equiv 3 \pmod 8 \implies 5q \equiv 4 \pmod 8 \implies q \equiv 4 \pmod 8.$$

Thus, $q = 8r + 4$ for some integer r, which implies that

$$11^{2011} = 125q + 111 = 125(8r + 4) + 111 = 1000r + 500 + 111 \implies 11^{2011} \equiv 611 \pmod{1000}.$$

Therefore, hundreds digit is $\boxed{6}$. ■

Remark. Don't forget your roots! We started off our modular arithmetic portion of this week by using the binomial theorem to solve the following problem:

What is the remainder when 6^{2020} is divided by 5?

Can we do something similar for the previous example?

The point is to not get sucked too deep in the rabbit hole that is modular arithmetic. It's easy to get caught up in all of the calculations and numbers that are involved. If you are doing a contest and modular arithmetic seems too bashy/time consuming, think of other ways to approach the problem!

§19.3.1 Exercises for this section

Exercise 19.25. Find the last two digits of $19^{20^{21^{22}}}$.

Exercise 19.26. Find the remainder when 12345^{67890} is divided by 999.

Exercise 19.27. Find the smallest positive value of x such that $2^x \equiv 2^{123} \pmod{65}$.

Exercise 19.28. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ if a and b are relatively prime positive integers. Verify that this congruence holds when $a = 15$ and $b = 14$.

§19.4 Challenging examples

Example 19.29. Find the last two non-zero digits of 2020!.

Solution. First, we must find the number of trailing zeroes in 2020!. The number of trailing zeroes is equal to the greatest power of 10 that divides 2020!. Since there are more powers of 2 than powers of 5 among the integers from 1 to 2020, the highest power of 5 dividing 2020! should equal the highest power of 10 that divides 2020!.
Here, we can use Legendre's formula for $p = 5$.

$$f(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor.$$

This will give us the number of trailing zeroes in the expression $n!$.

Remark. In general, for a prime p and n, Legendre's formula gives that the number of factors of p in $n!$ is

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

You can think of each term $\left\lfloor \frac{n}{p^k} \right\rfloor$ as counting the number of integers less than n divisible by p^k. It's easy to see that the number of factors of p in $n!$ is simply the number of integers less than n divisible by p, plus the number of integers less than n divisible by p^2, and so on; this is because if an integer between 1 and n inclusive has highest power k of the prime factor p, then we count it once each time we are counting numbers divisible by p^i for $1 \leq i \leq k$, meaning we count all k factors in total. This is the reasoning for Legendre's formula.

Hence, we find that the number of trailing zeroes in 2020! is

$$\left\lfloor \frac{2020}{5} \right\rfloor + \left\lfloor \frac{2020}{25} \right\rfloor + \left\lfloor \frac{2020}{125} \right\rfloor + \left\lfloor \frac{2020}{625} \right\rfloor = 404 + 80 + 16 + 3 = 503.$$

Therefore, the expression $\frac{2020!}{10^{503}}$ represents 2020! with no trailing zeroes. In order to find the last two digits of $\frac{2020!}{10^{503}}$, we take the expression mod 100. However, we note that it is much easier to find $\frac{2020!}{10^{503}}$ in mod 4 and mod 25 and then combine the equations using Chinese Remainder Theorem.
We will first consider $\frac{2020!}{10^{503}} \pmod{25}$. Let $z = \frac{2020!}{5^{503}}$. Note that $\frac{2020!}{10^{503}}$ is equivalent to $\frac{z}{2^{503}}$. Additionally, note that z is the same as saying all the factors of 2020! that are multiples of 5 have been divided through by their highest power of 5. I.e.

$$z = (1 \cdot 2 \cdot 3 \cdot 4 \cdot 1) \cdot (6 \cdot 7 \cdot 8 \cdot 9 \cdot 2) \ldots (2016 \cdot 2017 \cdot 2018 \cdot 2019 \cdot 404)$$

We will split these factors into sets based on the highest power of 5 they were divisible by. For example, since $75 = 3 \cdot 5^2$, 3 belongs in the 5^2 set

$$5^0 : \{1, 2, 3, 4, 6, 7, 8, 9, \ldots, 2016, 2017, 2018, 2019\}$$
$$5^1 : \{1, 2, 3, 4, 6, 7, 8, 9, \ldots 401, 402, 403, 403\}$$
$$5^2 : \{1, 2, 3, 4, 6, 7, 8, 9, \ldots 76, 77, 78, 79\}$$
$$5^3 : \{1, 2, 3, 4, 6, 7, 8, 9, \ldots 16\}$$
$$5^4 : \{1, 2, 3\}$$

Interestingly, $1 \cdot 2 \cdot 3 \cdot 4 \equiv -1 \pmod{25}$ and $6 \cdot 7 \cdot 8 \cdot 9 \equiv -1 \pmod{25}$. In fact, every 4 consecutive numbers starting from 1 has a product of -1 mod 25. We can prove this by representing the four consecutive numbers as $5z + 1, 5z + 2, 5z + 3$, and $5z + 4$ and expanding and taking mod 25. Therefore, let us group them into 4 consecutive numbers.

$$5^0 : \{(1, 2, 3, 4), (6, 7, 8, 9), \ldots, (2016, 2017, 2018, 2019)\}$$
$$5^1 : \{(1, 2, 3, 4), (6, 7, 8, 9), \ldots (401, 402, 403, 404)\}$$
$$5^2 : \{(1, 2, 3, 4), (6, 7, 8, 9), \ldots (76, 77, 78, 79)\}$$
$$5^3 : \{(1, 2, 3, 4), (6, 7, 8, 9), \ldots 16\}$$
$$5^4 : \{1, 2, 3\}$$

Since we only care about the product mod 25, we can substitute each group with -1. The 5^0 set has 404 groups, so its product is $(-1)^{404} = 1$. Similarly, the product of the sets denoted by $5^1, 5^2, 5^3$, and 5^4 are -1, 1, -16, and 6 respectively. Taking the product of each of these sub-products, we find that $z \equiv 96 \equiv 21 \pmod{25}$. We also have that $2^{-503} \equiv 2^{-3} \equiv 22 \pmod{25}$ by Euler's theorem. Therefore, $\frac{2020!}{10^{503}} \equiv 21 \cdot 22 \equiv 12 \pmod{25}$.

Thankfully the process to find $\frac{2020!}{10^{503}} \bmod 4$ is much quicker. Simply note that because there are far more powers of 2 than powers of 5 in the prime factorization of 2020!, $2^{505} | 2020!$. Therefore, $4 | \frac{2020!}{10^{503}}$, so $\frac{2020!}{10^{503}} \equiv 0 \pmod{4}$.

Finally, we have arrived at two congruences

$$\begin{aligned} \frac{2020!}{10^{503}} &\equiv 12 \pmod{25} \\ \frac{2020!}{10^{503}} &\equiv 0 \pmod{4}, \end{aligned}$$

which we can combine using the Chinese Remainder Theorem to get $\frac{2020!}{10^{503}} \equiv \boxed{12} \pmod{100}$ This example shows how the Chinese Remainder Theorem can be used in order to break down difficult problems in simpler, more managaeble ones. ■

Example 19.30. Find the last three digits of 7^{8^9}.

Solution. By this point, you should automatically think of modulo 1000 when it asks about the last three digits. To reduce the size of the numbers, we split up the problem into modulo 8 and modulo 125. Nothing new so far. Let's do modulo 8 first. We have $7 \equiv -1 \pmod{8}$, which implies that

$$7^{8^9} \equiv (-1)^{8^9} \equiv 1 \pmod{8}.$$

Now for modulo 125. By Euler's, we have $7^{\phi(125)} \equiv 1 \pmod{125}$, where $\phi(125) = 125\left(1 - \frac{1}{5}\right) = 100$.

Now, we need to find the remainder when 8^9 is divided by 100. We can't use Euler's right away, because $\gcd(8, 100) \neq 1$, so we split it up into modulo 4 and modulo 25. For modulo 4, we have

$$8^9 \equiv 0 \pmod{4}.$$

By Euler's, we have $8^{\phi(25)} \equiv 1 \pmod{25}$, where $\phi(25) = 25\left(1 - \frac{1}{5}\right) = 20$. This does not help us at all, because we want to find $8^9 \pmod{25}$, but Euler's tells us about 8^{20} instead. To proceed, we write $8^9 = \left(2^3\right)^9 = 2^{27}$. By changing this exponent to have a smaller base, we can get Euler's to tell us something useful now. Using the theorem again, we have

$$2^{\phi(25)} \equiv 2^{20} \equiv 1 \pmod{25} \implies 2^{27} \equiv 2^7 \equiv 3 \pmod{25}.$$

Hence,

$$\begin{aligned} 8^9 &\equiv 0 \pmod{4} \\ 8^9 &\equiv 3 \pmod{25}, \end{aligned}$$

so $8^9 \equiv 28 \pmod{100}$. It follows that

$$7^{8^9} \equiv 7^{28} \pmod{125}.$$

Now is the hard part. There's really no nice way to find this, except for to bash. However, there are different methods of bashing, the most efficient of which is **binary exponentiation.** Suppose you want to find $a^x \pmod{n}$, for some large x. We write x in its base two representation, and repeatedly square a, then reduce it mod n. For this example, we have $28 = 16 + 8 + 4$ and

$$\begin{aligned}
7^1 &\equiv 7 \pmod{125} \\
7^2 &\equiv 49 \pmod{125} \\
7^4 &\equiv \left(7^2\right)^2 \equiv 49^2 \equiv 2401 \equiv 26 \pmod{125} \\
7^8 &\equiv \left(7^4\right)^2 \equiv 26^2 \equiv 676 \equiv 51 \pmod{125} \\
7^{16} &\equiv \left(7^8\right)^2 \equiv 51^2 \equiv 2601 \equiv 101 \pmod{125}.
\end{aligned}$$

Therefore, $7^{28} \equiv 7^{16}7^87^4 \equiv 101 \cdot 51 \cdot 26 \equiv 5151 \cdot 26 \equiv 26 \cdot 26 \equiv 51 \pmod{125}$. We're left with one final system of congruences:

$$\begin{aligned}
7^{8^9} &\equiv 1 \pmod{8} \\
7^{8^9} &\equiv 51 \pmod{125}.
\end{aligned}$$

We can write $7^{8^9} = 125q + 51$ for some integer q and plug it into our first congruence to get

$$7^{8^9} \equiv 125q + 51 \equiv 5q + 3 \equiv 1 \pmod{8} \implies q \equiv 6 \pmod{8} \implies q = 8r + 6,$$

for some integer r. Finishing, we have

$$7^{8^9} = 125q + 51 = 125(8r + 6) + 51 = 1000r + 801,$$

so the last three digits are $\boxed{801}$. ■

§19.5 Homework Problems

Problem 19.1 (MATHCOUNTS)**.** [4] Find the least positive integer that leaves a remainder of 3 when divided by 5, a remainder of 7 when divided by 9, and a remainder of 7 when divided 13.

Problem 19.2 (MATHCOUNTS)**.** [4] For each positive integer n, $a_n = 9n+2$ and $b_n = 7n+3$. If the values common to both sequences are written as a sequence, the n^{th} term of that sequence can be expressed as $pn + q$, for integers p and q. What is the value of $p - q$?

Problem 19.3 (ARML 2002)**.** [6] Let a be an integer such that $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{23} = \frac{a}{23!}$. Find the remainder when a is divided by 13.

Problem 19.4 (2002 AIME II)**.** [7]It is known that, for all positive integers k,
$1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$. Find the smallest positive integer k such that $1^2 + 2^2 + 3^2 + \ldots + k^2$ is a multiple of 200.

Problem 19.5 (Dennis Chen)**.** [7] Let $p > 3$ be a prime number. Find the remainder when $(1^3)(1^3 + 2^3)(1^3 + 2^3 + 3^3) \cdots (1^3 + 2^3 + 3^3 \cdots + (p-2)^3)$ is divided by p.

Problem 19.6 (1989 AIME)**.** [8] One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.

Problem 19.7 (2019 AIME I)**.** [8] Find the least odd prime factor of $2019^8 + 1$.

Problem 19.8 (2012 AIME II)**.** [8] For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $\{3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \dots\}$. Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe and 13-safe.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.

20 Diophantine Equations, Bases

§20.1 Diophantine Equations

A **Diophantine equation** is an equation where we only seek integer solutions; like normal equations, diophantine equations will often come in systems. We often use techniques in both algebra and number theory to solve these equations.

Example 20.1. Find all integers (x, y) such that $3x + 2y = 5$.

Solution. Since we are looking for integer solutions, this is a Diophantine equation. At first glance, this equation has infinitely many solutions across the integers, and an obvious solution is $(1, 1)$.

In order to find the other solutions, we can build off of the first solution we found, $(1, 1)$. Since we are dealing with the expression $3x + 2y$, it becomes clear that x increases when y decreases, and vice versa. Now, we just need to find the specific balance between x and y to solve for the remaining solutions.

Observe that the GCD of 2 and 3 is 6. Applying this, we have that $3(x+2)+2(y-3) = 3x+2y$. We can take our original solution $(1, 1)$ and repeatedly add 2 to x and subtract 3 from y (and vice versa) to obtain our infinite solutions.

Thus, our solutions are in the form of $(1 + 2a, 1 - 3a)$ for all integers a. Plugging this in to our original equation, we have that $3(1 + 2a) + 2(1 - 3a) = 3 + 2 + 6a - 6a = 5$, so it does work. ■

Exercise 20.2. Does the equation $2x + 6y = 11$ have any integer solutions?

Example 20.3. Find all integers (x, y) such that $x^2 + 3x + 1 = 3y^2$.

Solution. Notice that there is a coefficient of 3 on both sides of the equation. This motivates us to take the equation $\mod 3$. Doing so gives us, $x^2 + 1 \equiv 0 \mod 3$ which becomes $x^2 \equiv 2 \mod 3$.However, a perfect square is never equivalent to $2 \mod 3$!

Let's prove this. Consider a number that is equivalent to $0 \mod 3$. Then squaring it will result in another number that is also $0 \mod 3$. Now consider a number $1 \mod 3$. Squaring it results in another number $1 \mod 3$. Finally, consider a number that is $2 \mod 3$. When we square it, it becomes a number $4 \mod 3 \to 1 \mod 3$. Thus, we have for all perfect squares x^2, $x^2 \equiv 0, 1 \mod 3$.

This contradicts with our solution that $x^2 \equiv 2 \mod 3$, so our original equation has no integral solutions. ■

In the next example, we will introduce Simon's Favorite Factoring Trick which is a powerful way to factor certain equations.

Example 20.4. Find all integer solutions (x, y) such that $xy = x + y$

Solution. After doing a bit of guess and check, we find that $(2, 2)$ amd $(0, 0)$ are valid solutions, and there don't seem to be any other solutions.

However, this is a bit unsatisfying because we don't know for sure whether these were the only solutions. Let's actually solve it.

Moving the x and y to the LHS, we have that

$$xy - x - y = 0$$

It's not clear how to proceed from here, but we might think to factor out an x which gives us

$$x(y-1) - y = 0$$

We would be able to factor this expression if we had $x(y-1) - (y-1) = 0$, but there's no constant term for us to do so. However, notice that we can add one to both sides to achieve this factorization! We now have

$$\begin{aligned} x(y-1) - y &= 0 \\ x(y-1) - y + 1 &= 1 \\ x(y-1) - (y-1) &= 1 \\ (x-1)(y-1) &= 1 \end{aligned}$$

Since we seek integer solutions, $(x-1)$ and $(y-1)$ must both be factors of 1. We either have that $x - 1 = y - 1 = 1$ or that $x - 1 = y - 1 = -1$. Thus, our two solutions are $(2, 2)$ and $(0, 0)$. ■

Now let's look at an example where our coefficients are not 1.

Example 20.5. Find all integer solutions (x, y) such that $2xy - 5y - 8x = -13$

Solution. Factoring out the y, we have that $y(2x-5) - 8x = -13$. Remembering what we did in the previous problem, we seek to add some constant c to both sides such that we are able to factor out a $(2x - 5)$ from $(-8x + c)$. Notice that $-4(2x - 5) = -8x + 20$. Thus, we wish to add 20 to both sides to be able to completely factor the LHS. We have that

$$\begin{aligned} 2xy - 5y - 8x &= -13 \\ y(2x-5) - 8x &= -13 \\ y(2x-5) - 8x + 20 &= 7 \\ y(2x-5) - 4(2x-5) &= 7 \\ (y-4)(2x-5) &= 7 \end{aligned}$$

Now, we just need to find the factors of 7 to solve for the values of x and y.

$7 = 7 \cdot 1 = (-7) \cdot (-1)$. However, these two factorizations each give us two cases to consider because we flip the order of $y - 4$ and $2x - 5$. Thus, we have four cases to consider.

$$\begin{aligned} 2x - 5 &= 7 \\ y - 4 &= 1 \end{aligned} \qquad \begin{aligned} 2x - 5 &= 1 \\ y - 4 &= 7 \end{aligned}$$

$$\begin{aligned} 2x - 5 &= -7 \\ y - 4 &= -1 \end{aligned} \qquad \begin{aligned} 2x - 5 &= -1 \\ y - 4 &= -7 \end{aligned}$$

Solving for (x, y), we have our desired solutions $(x, y) = (6, 5), (3, 11), (-1, 3), (2, -3)$. ■

Remark. The strategy we used in the previous two examples is known as **Simon's Favorite Factoring Trick**, or SFFT for short. Whenever we see some expression in the form of $xy + ax + by = c$, we add the constant ab to both sides so that we can factor the LHS expression into $(x+a)(x+b)$. The coefficient in front of the xy term will not always be 1, but the same idea can be applied.

Example 20.6 (AIME). Find $3x^2y^2$ if x and y are integers such that $y^2+3x^2y^2 = 30x^2+517$.

Solution. Moving all variables to the LHS, we get the equation $3x^2y^2 - 30x^2 + y^2 = 517$. Factoring out $3x^2$ from the first two terms, we have that $3x^2(y^2-10)+y^2 = 517$. Remembering SFFT, we can subtract 10 from both sides so that the LHS factors. Our equation now is

$$(3x^2 + 1)(y^2 - 10) = 507.$$

Since we have that x and y are both integers, we know that $3x^2+1$ and y^2-10 are both factors of 507. We have that $507 = 3 \cdot 13^2$. Notice that $3x^2 + 1 \equiv 1 \mod 3$. Thus, we can narrow our potential solutions to $3x^2 + 1 = 13$ or $3x^2 + 1 = 169$. Testing $3x^2 + 1 = 169$ does not yield an integer solution for x. However, we find that $3x^2 + 1 = 13$ and $y^2 - 10 = 39$ gives the valid solution of $(x, y) = (2, 7)$. Thus, $3x^2y^2 = 588$. ■

Exercise 20.7 (AHSME). How many ordered pairs (m, n) of positive integers are solutions to

$$\frac{4}{m} + \frac{2}{n} = 1?$$

Exercise 20.8. Let A, M, and C be digits with

$$(100A + 10M + C)(A + M + C) = 2005$$

What is A?

Now we'll work through a few more examples of Diophantine equations.

Example 20.9 (AHMSE). The number of triples (a, b, c) of positive integers which satisfy the simultaneous equations

$$ab + bc = 44$$
$$ac + bc = 23$$

is

Solution. As we have done in the previous examples, our first step here will be to factor both equations. Doing so gives us

$$b(a + c) = 44$$
$$c(a + b) = 23$$

Since we know that our variables are positive integers, we have that b and $a+c$ are both factors of 44 and that c and $a + b$ are both factors of 23.

Since 23 is prime, we have that either $c = 23$ or that $c = 1$. However, we can't have $c = 23$ because that implies that $a+b = 1$. If $a+b = 1$, a and b can't both be positive which contradicts with the "positive integers" condition of our problem.

Thus, we know that $c = 1$ and $a + b = 23$. Plugging in $c = 1$ to our first equation, we have that $ab + b = 44$. We also have that $a + b = 23$. Since we have ab, a, b terms between the two equations, we are motivated to add them and use SFFT.

Adding the two equations, we have that $ab + a + 2b = 67$. Factoring the a from the first two terms, we have $a(b + 1) + 2b = 69$. Adding 2 to both sides allows us to factorize the equation as $(a + 2)(b + 1) = 69$. Since we want positive a, b and remembering that $a + b = 23$, we have the two equations

$$\begin{aligned} a+2 &= 23 & \qquad a+2 &= 3 \\ b+1 &= 3 & \qquad b+1 &= 23 \end{aligned}$$

From this, we find our desired solutions $(a, b, c) = (21, 2, 1), (1, 22, 1)$. Thus, there are two ordered triples of positive integers that satisfy our original two equations. ■

Example 20.10 (Math League HS). What are all pairs of positive integers (a, b) for which $a^2 + b$ exceeds $a + b^2$ by 36?

Solution. We are given that $a^2 + b = a + b^2 + 36$. Moving all variables to the LHS, we have that $a^2 - b^2 + b - a = 36$. Notice that we can rewrite the LHS as

$$\begin{aligned} a^2 - b^2 + b - a &= 36 \\ (a+b)(a-b) - (a-b) &= 36 \\ (a+b-1)(a-b) &= 36 \end{aligned}$$

Thus, both $(a+b-1)$ and $(a-b)$ are factors of 36. Notice that $a+b-1 > a-b$ because when we rearrange this inequality, we get that $2b > 1$ which is always true since we are dealing with positive integers. Thus, we have four cases

$$\begin{aligned} a+b-1 &= 36 & \qquad a+b-1 &= 18 \\ a-b &= 1 & \qquad a-b &= 2 \end{aligned}$$

$$\begin{aligned} a+b-1 &= 12 & \qquad a+b-1 &= 9 \\ a-b &= 3 & \qquad a-b &= 4 \end{aligned}$$

Solving these equations, we actually find 3 solutions because the set of equations $a + b - 1 = 18, a - b = 2$ does not give us integer solutions. Our desired solutions are $(x, y) = (19, 18), (8, 5), (7, 3)$. ■

The main strategies behind solving Diophantine equations are either finding ways to factorize the original equation(s), or taking the equation $\mod n$ to simplify it. Additionally, if we have fractions or square roots, find ways to get rid of them perhaps by multiplying or squaring both sides.

Exercise 20.11 (AMC 10). In multiplying two positive integers a and b, Ron reversed the digits of the two-digit number a. His erroneous product was 161. What is the correct value of the product of a and b?

Exercise 20.12 (PUMaC). If p, q, and r are primes with $pqr = 7(p + q + r)$, find $p + q + r$.

§20.2 Bases

Definition 20.13. A **base** is a system of writing numbers. Our familiar number system uses base-10. Take the number 237, for example. What do the digits 2, 3, and 7 represent in base-10? They signify that

$$237 = 2 \cdot 10^2 + 3 \cdot 10 + 7$$

In general, a base-b number $a_n a_{n-1} a_{n-2} \dots a_0$, where the digits a_i are nonnegative integers less than b (with $a_n > 0$, has the value

$$\sum_{i=0}^{n} a_i b^i = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_0$$

This notation may look slightly intimidating, but bases will make a lot more sense after looking at some examples. Notation-wise, if a number is not written in base-10, we write the base as a subscript. For example, 324_5 denotes 324 in base-5. For base-10, the subscript may also be used for clarification.

Example. Convert 231_5, 1111_2 and 321_9 to their base-10 equivalent.

Solution.

$$\begin{aligned} 231_5 &= 2 \cdot 5^2 + 1 \cdot 5^2 + 1 = 56_{10} \\ 1111_2 &= 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 = 15_{10} \\ 321_9 &= 3 \cdot 9^2 + 2 \cdot 9 + 1 = 262_{10} \end{aligned}$$

■

Example. Convert 59 to base-16.

Solution. We can do this by looking for the leading digit, then working our way down. $59 < 256$, so the first digit occurs in the "16" column. $59 = 3 \cdot 16 + 11$. Thus, we have $59_{10} = 3B_{16}$. ■

Something to note is that the **digits used in base-b are the digits 0→ b-1**. For example, in base-10, we used the digits $0 \to 9$. For bases higher than 10, digits greater than 9 are usually denoted using letters of the alphabet starting from A=10. For example, in hexadecimal (base-16), we use A, B, C, D, E, and F to represent 10, 11, 12, 13, 14, and 15, respectively.

Operating on numbers in a different base system follows the same general idea as operating on numbers in base 10, except that "carrying" happens with respect to the base and not 10. Let's look at some examples:

Example. What is the sum of 476_8 and 321_8?

Solution.
$$\begin{array}{r} 476_8 \\ +321_8 \\ \hline 1017_8 \end{array}$$

This addition was done similar to how it is normally done, except that we "carried" over with respect to 8. $6 + 1 = 7$ in the last column is done as normal. In the second-to-last

column, $7+2=9_{10}=11_8$, so a 1 is placed down and a 1 is carried over. Then, we have $4+3+1=8_{10}=10_8$. Thus, the total is 1017_8. ■

Example. What is the product of 26_8 and 21_8?

Solution.
$$\begin{array}{r} 26_8 \\ \times 21_8 \\ \hline 26_8 \\ +540_8 \\ \hline 566_8 \end{array}$$

Similarly, we can use normal multiplication procedures but just carry over at different values. Multiply $1 \times 26 = 26_8$ as normal, but $26_8 \times 2 = 54_8$ because we carry over at 8 instead. Then, addition proceeds as normal, where we get 566_8 as a result.

■

Another way to operate on numbers in a different base system is to convert everything to base-10, operate normally, then convert them back. The method is a matter of personal preference, although competition problems rarely involve more than a few operations.

Bases frequently show up in both AMC and AIME problems, and base problems are often simply diophantine equations in disguise.

Example 20.14 (AHSME). Let the product $(12)(15)(16)$, each factor written in base b, equals 3146 in base b. Let $s = 12+15+16$, each term expressed in base b. Then s, in base b, is **(A)** 43 **(B)** 44 **(C)** 45 **(D)** 46 **(E)** 47

Solution. We can convert 12_b, 15_b, 16_b, 3146_b to base-10.

$$\begin{aligned} 12_b &= b+2 \\ 15_b &= b+5 \\ 16_b &= b+6 \\ 3146_b &= 3b^3+b^2+4b+6 \end{aligned}$$

Plugging these conversions back into the original equation, we get

$$\begin{aligned} (b+2)(b+5)(b+6) &= 3b^3+b^2+4b+6 \\ b^3+13b^2+5b+60 &= 3b^3+b^2+4b+6 \\ 2(b^3-6b^2-24b-27) &= 0 \end{aligned}$$

By the Rational Root Theorem, we know that b must divide 27. Furthermore, we must have $b \geq 7$ because the digit 6 is valid in base b. The only factors of 27 that satisfy this criteria are 9 and 27. 27 appears much too large to be a root of the cubic, so $b=9$ (this can also be verified through computation). Thus, $s = 12_9+15_9+16_9 = B)44_9$ ■

Example 20.15 (2018 AIME I). The number n can be written in base 14 as $\underline{a}\ \underline{b}\ \underline{c}$, can be

written in base 15 as $\underline{a}\ \underline{c}\ \underline{b}$, and can be written in base 6 as $\underline{a}\ \underline{c}\ \underline{a}\ \underline{c}$, where $a > 0$. Find the base-10 representation of n.

Solution. Let's first convert the given numbers to base 10. Since n is $\underline{a}\ \underline{b}\ \underline{c}_{14}$, we have that

$$n = a \cdot 14^2 + b \cdot 14 + c = 196a + 14b + c$$

Converting $\underline{a}\ \underline{c}\ \underline{b}_{15}$ and $\underline{a}\ \underline{c}\ \underline{a}\ \underline{c}_6$ similarly, we get the two equations

$$n = 225a + 15c + b$$
$$n = 222a + 37c$$

Setting the above two equations equal to each other,

$$225a + 15c + b = 222a + 37c$$
$$22c = 3a + b$$

Since c is nonzero, we know that $3a + b = 22c \geq 22$. Also, a is a digit in base 6 and b is a digit in base 14, so $a \leq 5$ and $b \leq 13$. Therefore, $22 \leq 3a + b \leq 28$. So the only possibility is $c = 1$. Then, we have

$$3a + b = 22$$

Subtracting the first and second equation and plugging in $c = 1$, we get

$$196a + 14b + c = 225a + 15c + b$$
$$13b = 29a + 14c$$
$$13b = 29a + 14$$

Then, we can easily solve for a and b through guess and check because a, b are integers with a limited range. We get $a = 4$ and $b = 10$. Plugging a, b, and c into one of the original expressions gives $196a + 14b + c = 925$. ■

Remark. It is a common technique to convert numbers written in other bases to base-10 for ease of comparison.

Example 20.16 (2020 AIME I). A positive integer N has base-eleven representation $\underline{a}\underline{b}\underline{c}$ and base-eight representation $\underline{1}\underline{b}\underline{c}\underline{a}$, where a, b, and c represent (not necessarily distinct) digits. Find the least such N expressed in base ten.

Solution. First, convert both numbers to base-10 in terms of the variables so that they can be compared easily. We have

$$\underline{a}\underline{b}\underline{c}_{11} = 121a + 11b + c$$
$$\underline{1}\underline{b}\underline{c}\underline{a}_8 = 512 + 64b + 8c + a$$

Equating the two,

$$121a + 11b + c = 512 + 64b + 8c + a$$
$$120a = 512 + 53b + 7c$$

Notice $N = 121a + 11b + c$, so we can start by minimizing the variable a. Minimizing a minimizes N because a is the leading digit when expressing N in base-11. Variables a, b, c must all be positive, so the RHS of

$$120a = 512 + 53b + 7c$$

is at least 512. Therefore, the minimum value of a is 5. Now, we can test if b, c can have appropriate values if $a = 5$. Plugging in $a = 5$, we get

$$600 = 512 + 53b + 7c$$
$$88 = 53b + 7c$$

Then, we continue by trying to minimize b because b is the next digit in the base-11 representation of N. Letting $b = 0$ clearly won't work, so we try $b = 1$. If b=1,

$$88 = 53(1) + 7c$$
$$35 = 7c$$
$$5 = c$$

Variable c works out to be an integer, which is exactly what we hoped for. Thus, the solution is

$$N = 121a + 11b + c = 5 \cdot 121 + 11 \cdot 1 \cdot 5$$
$$= 605 + 11 + 5 = 621$$

■

§20.3 Homework Problems

Problem 20.1 (Purple Comet HS 2004)**.** [4] Find n such that $n-76$ and $n+76$ are both cubes of positive integers.

Problem 20.2 (2017 AIME I)**.** [5] A rational number written in base eight is $\underline{ab}.\underline{cd}$, where all digits are nonzero. The same number in base twelve is $\underline{bb}.\underline{ba}$. Find the base-ten number $\underline{abc}$.

Problem 20.3 (2015 AMC 10)**.** [5] Hexadecimal (base-16) numbers are written using numeric digits 0 through 9 as well as the letters A through F to represent 10 through 15. Among the first 1000 positive integers, there are n whose hexadecimal representation contains only numeric digits. What is the sum of the digits of n?

Problem 20.4 (1987 AIME)**.** [6] Find $3x^2y^2$ if x and y are integers such that $y^2 + 3x^2y^2 = 30x^2 + 517$.

Problem 20.5 (2014 AMC 12)**.** [6] There are exactly N distinct rational numbers k such that $|k| < 200$ and

$$5x^2 + kx + 12 = 0$$

has at least one integer solution for x. What is N?

Problem 20.6 (2008 AIME I)**.** [6] There exist unique positive integers x and y that satisfy the equation $x^2 + 84x + 2008 = y^2$. Find $x + y$.

Problem 20.7 (2013 AMC 10A)**.** [6] In base 10, the number 2013 ends in the digit 3. In base 9, on the other hand, the same number is written as $(2676)_9$ and ends in the digit 6. For how many positive integers b does the base-b-representation of 2013 end in the digit 3?

Problem 20.8 (2019 AMC 10)**.** [6] For some positive integer k, the repeating base-k representation of the (base-ten) fraction $\frac{7}{51}$ is $0.\overline{23}_k = 0.232323...{}_k$. What is k?

Problem 20.9 (2013 AMC 10)**.** [7] Bernardo chooses a three-digit positive integer N and writes both its base-5 and base-6 representations on a blackboard. Later LeRoy sees the two numbers Bernardo has written. Treating the two numbers as base-10 integers, he adds them to obtain an integer S. For example, if $N = 749$, Bernardo writes the numbers 10,444 and 3,245, and LeRoy obtains the sum $S = 13{,}689$. For how many choices of N are the two rightmost digits of S, in order, the same as those of $2N$?

Problem 20.10 (2003 AIME I)**.** [8] Let N be the number of positive integers that are less than or equal to 2003 and whose base-2 representation has more 1's than 0's. Find the remainder when N is divided by 1000.

Provide a detailed solution, or explain what progress you made, even if you didn't get an answer.